МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра комп'ютерних наук

«До захисту допущено»
В.о. завідувача кафедри
_____ Ігор ШЕЛЕХОВ
(підпис)
18 грудня 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістр

зі спеціальності 122 - Комп'ютерних наук,
освітньо-наукової програми «Інформатика»
на тему: «Інформаційні технології та інструменти активних дій в кібербезпеці»
здобувача групи ІН.м-22 Ященко Анни Миколаївни

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Анна ЯЩЕНКО
(підпис)

Керівник,
в.о. завідувача кафедри,
кандидат технічних наук, доцент Ігор ШЕЛЕХОВ _____
(підпис)

Суми – 2023

Сумський державний університет

Факультет електроніки та інформаційних технологій

Кафедра комп'ютерних наук

«Затверджую»

В.о. завідувача кафедри

_____ Ігор ШЕЛЕХОВ

(підпис)

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр

зі спеціальності 122 - Комп'ютерних наук, освітньо-наукової програми «Інформатика»

здобувача групи ІН.м-22 Ященко Анни Миколаївни

1. Тема роботи: «Інформаційні технології та інструменти активних дій в кібербезпеці» затверджую наказом по СумДУ від «06» грудня 2023 року № 1412-VI.
2. Термін здачі здобувачем кваліфікаційної роботи до 18 грудня 2023 року_____
3. Вхідні дані до кваліфікаційної роботи _____
4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити) *1)* Аналіз проблеми предметної області, постановка й формування завдань дослідження. *2)* Огляд технологій, що використовуються в інформаційних технологіях та інструментах активних дій.

3) Виконання практичної частини.

4) Аналіз результатів.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)_____
6. Консультанти до проекту (роботи), із значенням розділів проекту, що стосується їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ Керівник _____

(підпис) (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	Аналіз проблеми предметної області, постановка й формування завдань дослідження		
2	Огляд методів, інформаційних технологій та програмного забезпечення активних дій в кібербезпеці		
3	Застосування програмних продуктів для вирішення задачі		
4	Аналіз отриманих результатів		
5	Оформлення пояснювальної записки до кваліфікаційної роботи		

Здобувач вищої освіти _____ Керівник _____

(підпис) (підпис)

АНОТАЦІЯ

Записка: 61 стор., 39 рис., 2 табл., 22 джерела.

Обґрунтування актуальності теми роботи – розвиток та застосування інформаційних технологій для активних дій у кібербезпеці є вкрай важливим для захисту від кіберзагроз, що мають властивість постійно вдосконалюватись та еволюціонувати.

Об’єкт дослідження — інформаційні технології та програмно-технічне забезпечення активних дій в кібербезпеці.

Предмет дослідження – реалізація інформаційних технологій для виконання завдань активних дій в кібербезпеці.

Мета роботи — дослідження та аналіз сучасних інструментів активних дій в кібербезпеці, оцінка їх технічної можливості та ефективності в реальних умовах, аналіз програмного інструментарію і його впровадження.

Методи дослідження — аналіз наукових публікацій, статистичний аналіз, а також порівняльний аналіз різних підходів в кібербезпеці.

Результати — результати дослідження підкреслюють важливість активних заходів у захисті цифрових середовищ та пропонують рекомендації для їх покращення та ефективного застосування.

ІНФОРМАЦІЙНА СИСТЕМА, АКТИВНІ ДІЇ, ПАСИВНИЙ ТА АКТИВНИЙ ЗАХИСТ, IPS/IDS, SIEM-СИСТЕМИ, WAZUH, ZENMAP

ЗМІСТ

ВСТУП

Актуальність. Сучасний світ дедалі більше залежить від цифрових технологій, що підвищує важливість кібербезпеки. Розвиток та застосування інформаційних технологій для активних дій у кібербезпеці є важливим для захисту від розвинутих кіберзагроз.

Об'єкт дослідження. Кіберпростір, зокрема, інформаційні системи та мережеві структури, які потребують захисту від кіберзагроз.

Предмет дослідження. Методи та інструменти активних дій у кібербезпеці, їх застосування та вплив на загальну безпеку інформаційних систем.

Гіпотеза. Ефективне використання інформаційних технологій для активних дій у кібербезпеці може значно покращити захист від сучасних кіберзагроз.

Наукова новизна. Дослідження вносить вклад у розробку стратегій кібербезпеки, акцентуючи на значенні активних дій та використанні передових технологій для протидії кіберзагрозам.

Структура. Робота включає аналіз існуючих підходів у кібербезпеці, огляд інструментів активного захисту, оцінку їх ефективності, розробку методологічного підходу, аналіз потенційних ризиків, формування рекомендацій, та висновки.

1 ІНФОРМАЦІЙНИЙ ОГЛЯД

1.1 Сучасні загрози в кібербезпеці

В наш час, коли технології стрімко розвиваються та переплітаються з усіма сферами нашого життя, питання кібербезпеки стає фундаментальним елементом цифрового простору. Ера високорозвинених технологій принесла безліч новаторських можливостей, однак разом із цим вона відкрила двері для ряду складних та непередбачуваних загроз.

Цифровий світ на сьогоднішній день пронизаний підключеними мережами, які об'єднують людей, компанії та держави. Ця взаємодія, хоча й розширює можливості спілкування та обміну інформацією, але також вносить ризики. Індивіди, які залежать від технологій для роботи, навчання та розваг, стають вразливими перед кіберзагрозами.

Кіберзагрози – це наявні та потенційно можливі явища і чинники, що створюють небезпеку інтересам людини, суспільства та держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об’єктах національної інформаційної інфраструктури.

Кіберзагрози загалом можна класифікувати за наступними критеріями [1]:

1. За джерелом: зовнішні та внутрішні кіберзагрози.

Зовнішні кіберзагрози включають широкий спектр атак, які походять ззовні, від індивідів, груп, організацій або держав. Ці загрози можуть бути спрямовані на комп'ютерні системи, мережі, програмне забезпечення та дані з метою завдання шкоди, отримання конфіденційної інформації або викрадення ресурсів.

Приклади зовнішніх кіберзагроз:

- Хакерські атаки. Зовнішні хакери можуть намагатися отримати несанкціонований доступ до систем, використовуючи різноманітні техніки, такі як перехоплення паролів, експлойти вразливостей програмного забезпечення або атаки на слабкі сторони системи.

- Фішинг. Атаки фішингу полягають у виманюванні конфіденційної інформації, такої як паролі чи банківські дані, шляхом виглядання атакувачем як довірливого джерела.
- Віруси та Черв'яки. Зловмисний код може бути розповсюджений через заражені файли, електронні повідомлення або інші канали, призводячи до поширення вірусів чи черв'яків, які можуть завдати шкоди системам або використовувати їх для атаки інших систем.
- DDoS-атаки (атаки на доступ). Атаки, спрямовані на переповнення мережевих ресурсів чи служби, з метою робити їх недоступними для легітимних користувачів.
- Атаки на вразливості. Експлуатація вразливостей в програмному забезпеченні або операційних системах для незаконного доступу чи виконання шкідливих дій.
- Шпигунство (витік конфіденційної інформації). Атаки, спрямовані на витік або здобуття конфіденційної інформації, такої як комерційні секрети, клієнтська база чи стратегічні дані.
- Соціальний інжиніринг. Використання маніпуляційних та обманюючих методів для отримання доступу чи інформації від осіб всередині організації.

Внутрішні кіберзагрози виникають всередині організації та можуть бути пов'язані зі співробітниками або іншими внутрішніми факторами. Ці загрози можуть створювати серйозні проблеми для інформаційної безпеки.

Приклади внутрішніх кіберзагроз:

- Недбалість працівників. Ситуації, коли працівники можуть ненавмисно викликати проблеми безпеки, наприклад, втратити або неправильно обробити конфіденційну інформацію.
- Недостатня освіта з кібербезпеки. Відсутність у співробітників базового розуміння кібербезпеки може призвести до

необережного поводження з конфіденційною інформацією та підвищувати ризик атак.

- Несанкціонований доступ. Співробітники, які намагаються отримати несанкціонований доступ до даних або ресурсів, до яких вони не мають прав.
- Втрати або крадіжка пристроїв. Втрати чи крадіжка комп'ютерів, ноутбуків, смартфонів або інших пристроїв, які містять конфіденційну інформацію.
- Недбалість у зберіганні паролів. Використання слабких паролів чи недостатня охорона від доступу до облікових записів.
- Саботаж інсайдерів. Спроби співробітників навмисно завдати шкоди організації, розголошуючи конфіденційну інформацію чи вчиняючи інші деструктивні дії.
- Некоректне використання привілеїв. Використання владних або адміністративних привілеїв для несанкціонованого доступу чи внесення змін у системі.
- Неправильна конфігурація систем. Ненавмисна неправильна конфігурація мережевих пристроїв чи серверів, що може призвести до збою в безпеці.

2. За спрямованістю: шпигунські атаки, промислові, терористичні, цільові.

- Шпигунські атаки (Cyber Espionage) – є формою кіберзагроз, спрямованою на отримання конфіденційної інформації з метою вигоди або завдання шкоди. Головною метою шпигунських атак є отримання конфіденційної інформації. Атакуючі можуть використовувати широкий спектр засобів, таких як шкідливі програми, вразливості в програмному забезпеченні, соціальний інжиніринг тощо. Ці атаки можуть бути спрямовані на різні галузі, включаючи економіку, науку, технології, військові відомості, політику та інші.

- Промислові атаки (Industrial Espionage) – це вид кіберзагроз, спрямований на комп'ютерні системи та мережі промислових об'єктів, таких як заводи, енергетичні підприємства, транспортні системи, системи водопостачання та інші критичні інфраструктурні об'єкти. Промислові атаки можуть призвести до серйозних фізичних та економічних наслідків, включаючи призупинення виробництва, збої в постачанні електроенергії тощо.
- Терористичні атаки (Cyber Terrorism) – форма кіберзагроз, яка спрямована на створення паніки, завдання шкоди інфраструктурі або вплив на суспільно-політичну ситуацію. Кібертероризм може мати глобальний вплив, оскільки онлайн-середовище не обмежується межами країн або регіонів.
- Цільові атаки – атаки, що спрямовані на конкретну організацію, компанію чи особу з метою отримання конфіденційної інформації, завдання шкоди або реалізації інших кримінальних цілей.

3. За методами атаки: фішинг, шкідливе програмне забезпечення, експлойти, DoS та DDoS атаки, соціальний інжиніринг, людина посередині, фармінг.
   - Фішинг (Phishing) – атака, під час якої зловмисники використовують маскуючі електронні листи або веб-сайти, щоб отримати конфіденційну інформацію від користувачів;
   - Шкідливе програмне забезпечення (Malware) – включає в себе використання шкідливих програм, таких як віруси, троянські програми, черв'яки, для отримання несанкціонованого доступу або завдання шкоди;
   - Експлойти (Exploits) – програмний код або послідовність команд, які використовуються для використання вразливостей у

програмному чи апаратному забезпеченні з метою виконання атаки;

- DoS (Denial of Service) та DDoS (Distributed Denial of Service) атаки – види кібератак, спрямовані на перевантаження ресурсів системи чи мережі, щоб заборонити або обмежити доступ до них легітимним користувачам;
- Соціальний інжиніринг (Social Engineering) – метод використання маніпулювання психологічними факторами, який має на меті отримання конфіденційної інформації або здійснення несанкціонованих дій шляхом взаємодії з людьми та використання їх довіри;
- Людина посередині (Man-in-the-Middle Attack або MITM Attack) – тип кібератаки, під час якої зловмисник вставляє зловмисне обладнання між комунікуючими сторонами з метою перехоплення, зміни або блокування комунікації між ними;
- Фармінг (Pharming) – вид кібератаки, в ході якої зловмисники намагаються перенаправити легітимних користувачів на фальшиві веб-сайти, щоб збирати їхні конфіденційні дані, такі як імена користувачів, паролі або фінансову інформацію.

Для запобігання, попередження та реагування на кіберзагрози використовуються заходи пасивного та активного захисту в кібербезпеці.

1.2 Активний та пасивний захист в кібербезпеці

1.2.1 Активний захист у кібербезпеці

Активний захист в кібербезпеці є відносно новим та динамічним напрямком, який фокусується на превентивних та реактивних заходах для виявлення, запобігання та відповіді на кіберзагрози. Він передбачає не лише пасивне очікування атак, але й активну участь у виявленні та нейтралізації потенційних загроз.

Програмне забезпечення безпеки інформації та керування подіями (SIEM) є однією з найкращих інновацій у технології безпеки. Це включає процес збору, аналізу та реагування на події, пов’язані з безпекою, сповіщення та звіти. Він не зосереджується лише на одному питанні. Навпаки – він агрегує дії з усіх ресурсів організації, щоб виявити будь-які зловмисні дії в IT-інфраструктурі.

Незважаючи на те, що концепція SIEM відносно нова, вона була розроблена на основі двох уже існуючих технологій - управління подіями безпеки і управління інформацією про безпеку . SIEM — це програмне рішення, яке аналізує дані журналів і подій у режимі реального часу, щоб забезпечити кореляцію подій, моніторинг загроз і реагування на випадки. З іншого боку, SIEM збирає, аналізує та звітує про дані журналу [1].

Розширений обсяг цієї технології може бути досить складним для роботи та потребує навичок спеціалізованих IT-техніків. Тим не менш, кожна зацікавлена сторона в бізнесі чи організації повинна розуміти основи того, як SIEM впливає на підприємство.

Основною характеристикою активного захисту є моніторинг та аналіз мережевого трафіку у реальному часі. Це означає використання розширених систем виявлення вторгнень (IDS) та систем управління інцидентами безпеки (SIEM), які дозволяють швидко ідентифікувати підозрілу активність та вживати заходів для її блокування або усунення. На рис. 1.1 представлено основні компоненти SIEM.

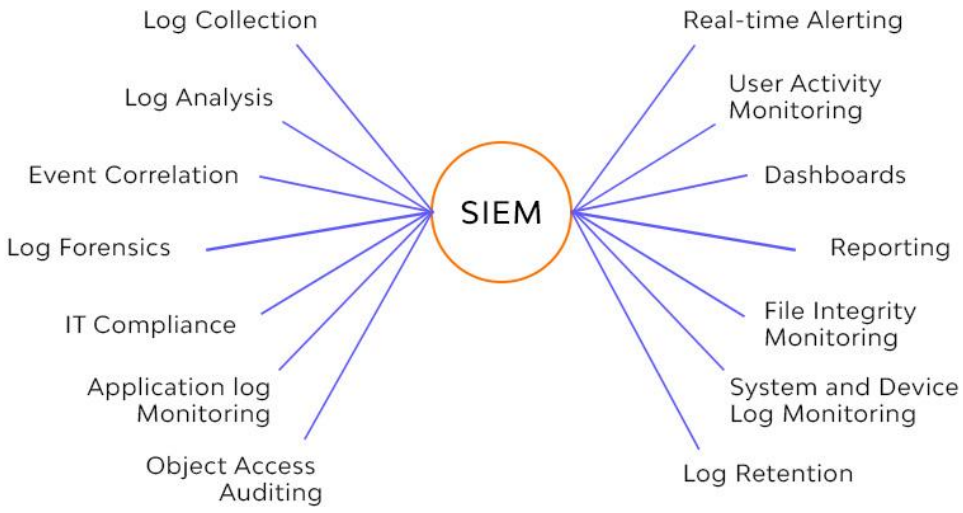


Рисунок 1.1 – Компоненти та можливості SIEM

Крім того, активний захист включає заходи з протидії кіберзагрозам, такі як Threat Hunting, де аналітики безпеки активно шукають ознаки компрометації всередині мережі, та відповідні контрзаходи на кібератаки. Це може включати в себе встановлення "медових горщиків" (honeypots) для виявлення та відстеження атакуючих, а також використання автоматизованих систем для швидкого реагування на інциденти. Схему роботи «Медових горщиків» представлено на рис. 1.2.

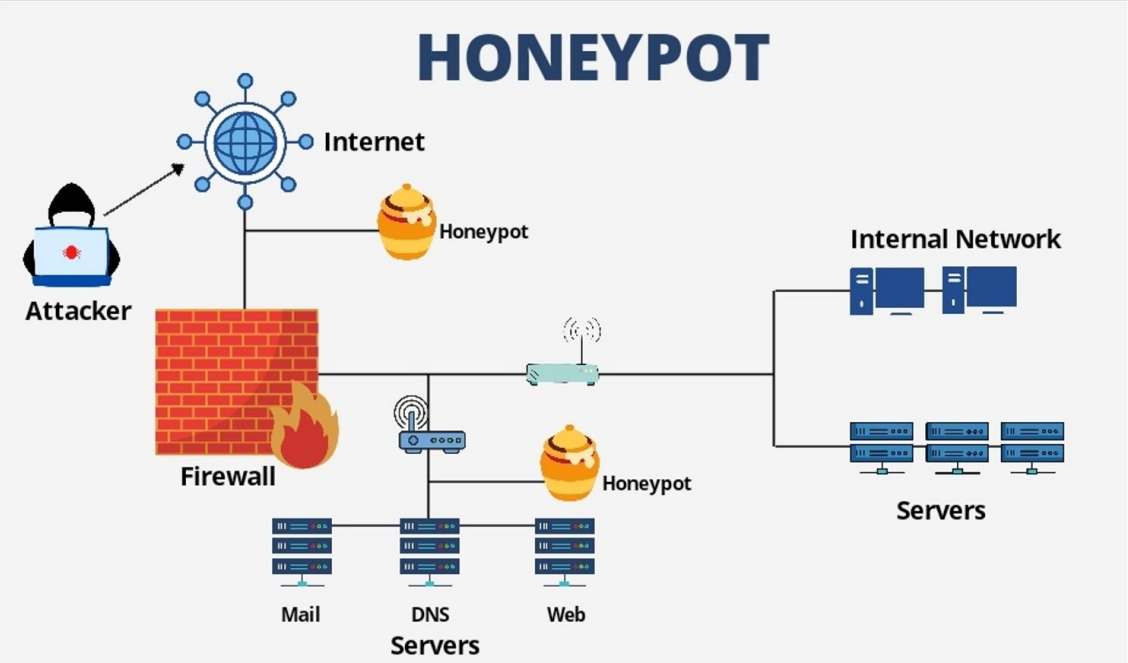


Рисунок 1.2 – Схема роботи "Медових горщиків" (HONEYPOTS)

Іншим важливим аспектом активного захисту є постійне оновлення та адаптація безпекових стратегій з урахуванням нових загроз та тенденцій у кіберзлочинності. Це включає регулярні тренінги для персоналу, щоб підвищити обізнаність про потенційні кіберзагрози та навчити ефективним методам протидії [2].

В цілому, активний захист в кібербезпеці є більш гнучким та агресивним підходом, який дозволяє не лише пасивно реагувати на кіберзагрози, але й активно виявляти та нейтралізувати їх, часто ще до того, як вони заподіяють шкоду. Це забезпечує більш комплексний та ефективний рівень захисту в постійно змінюваному кіберпросторі.

1.2.2 Пасивний захист у кібербезпеці

Пасивний захист у кібербезпеці відіграє важливу роль у забезпеченні безпеки інформаційних систем та мереж. Він полягає в створенні захисних бар'єрів, які мають на меті запобігти несанкціонованому доступу або втручанню у системи та дані [3]. Цей підхід до кібербезпеки зосереджений на попередженні атак шляхом встановлення захисних мір, таких як файрволи, антивірусне програмне забезпечення, шифрування даних, та інші засоби захисту.

Одним із ключових елементів пасивного захисту є регулярне оновлення безпекових протоколів та програмного забезпечення. Це дозволяє виявляти та запобігати вразливостям у системі, які можуть бути використані зловмисниками. Крім того, важливим аспектом є розробка та впровадження політик безпеки, які включають навчання персоналу, розробку правил поведінки у мережі, та контроль за дотриманням цих правил.

Пасивний захист також передбачає регулярне проведення аудитів безпеки та оцінок ризиків. Це включає аналіз потенційних загроз та вразливостей системи, а також розробку планів на випадок кібератак або інших інцидентів. Важливим є також резервне копіювання даних та підготовка планів відновлення після порушень, що дозволяє забезпечити цілісність та доступність інформації навіть у випадку успішної атаки.

Загалом, пасивний захист в кібербезпеці зосереджується на попередженні та мінімізації ризиків, не залучаючи активних дій проти атакуючих. Це створює надійний фундамент для захисту кіберпростору, однак часто не достатньо для протистояння складним та динамічним кіберзагрозам сучасності. Тому, хоча пасивний захист є необхідною складовою комплексної кібербезпеки, він часто доповнюється активними заходами.

1.2.3 Порівняльний аналіз захисту

Пасивний та активний захист у кібербезпеці відіграють критично важливі ролі в захисті інформаційних систем та мереж. Обидва підходи є

фундаментальними, але вони суттєво відрізняються за своїми методами, цілями та використанням. Розуміння цих відмінностей та їх правильне застосування є ключовим для створення комплексної та ефективної стратегії кібербезпеки.

Пасивний захист зосереджений на попередженні атак шляхом створення міцного оборонного бар'єру. Основна ідея полягає у запобіганні доступу несанкціонованих користувачів до системи або мережі. Типові пасивні заходи безпеки включають встановлення файрволів, використання антивірусного програмного забезпечення, застосування шифрування даних та імплементація систем контролю доступу. Ці інструменти фокусуються на мінімізації вразливостей до потенційних загроз, що дозволяє уникнути атак або хоча б зменшити їх вплив [4].

Пасивний захист також включає регулярні оновлення безпекових протоколів та програмного забезпечення, що дозволяє системі залишатися крок попереду потенційних кіберзагроз. Важливою складовою пасивної кібербезпеки є також розробка та впровадження політик безпеки, навчання співробітників та проведення аудитів та оцінок ризиків.

З іншого боку, активний захист в кібербезпеці має на меті не лише виявляти та запобігати атакам, але й активно відслідковувати та відповідати на них. Активні заходи безпеки включають моніторинг та аналіз мережевої активності в реальному часі, використання систем виявлення вторгнень та ведення кіберрозвідки. Ці дії дозволяють не лише виявляти існуючі загрози, але й прогнозувати потенційні атаки, а також здійснювати швидке реагування на інциденти.

Активний захист також включає розробку стратегій для відповіді на інциденти, включаючи плани відновлення після порушень та вироблення контрзаходів на кібератаки. Однією з ключових складових активного захисту є "мисливські" операції (cyber hunting), де фахівці з кібербезпеки активно шукають ознаки компрометації всередині мережі та вживають заходів для нейтралізації загроз.

При порівнянні пасивного та активного захисту, ключовим фактором є їх фокус. Пасивний захист зосереджений на попередженні та мінімізації ризиків, використовуючи заздалегідь встановлені бар'єри та правила. В той час як активний захист вимагає постійної уваги, аналізу та готовності до швидкого відповіді на загрози. Активні методи забезпечують більш гнучкий і агресивний підхід, що дозволяє ефективно реагувати на динамічно змінюване кіберзагрозове середовище.

В таблиці 1.1 представлено основні відмінності між активним та пасивним захистом в кібербезпеці.

Таблиця 1.1 – Основні відмінності між пасивним та активним захистом

Аспект	**Пасивний захист**	**Активний захист**
Підхід до захисту	Зосереджений на створенні бар'єрів та захисних мір для запобігання атак.	Часто автоматизований і не вимагає постійної уваги або втручання після налаштування.
Реагування на загрози	Спрямований на запобігання атакам та мінімізацію шкоди; рідше включає активні відповіді на атаки.	Орієнтований на швидке виявлення та реагування на атаки, часто в реальному часі.
Стратегія безпеки	Ґрунтується на стандартизованих та заздалегідь визначених правилах і політиках безпеки.	Орієнтований на швидке виявлення та реагування на атаки, часто в реальному часі.
Запобігання та виявлення	Переважно фокусується на запобіганні, використовуючи заздалегідь встановлені методи.	Включає методи виявлення та аналізу для ідентифікації невідомих або маловивчених загроз.
Залученість персоналу	Часто автоматизований і не вимагає постійної уваги або втручання після налаштування.	Вимагає неперервного моніторингу та втручання з боку спеціалістів кібербезпеки.

Загалом, ефективна стратегія кібербезпеки вимагає поєднання обох цих підходів. Пасивні заходи забезпечують солідний фундамент для оборони, тоді як активні методи дозволяють адаптуватися та реагувати на нові та

еволюціонуючі загрози. Разом вони формують комплексну систему захисту, яка здатна протистояти різноманітним викликам у світі кібербезпеки.

1.3 Основні методи вирішення задач в кібербезпеці

У сучасному цифровому світі, де обсяг та складність кіберзагроз невпинно зростають, ефективна кібербезпека вимагає комплексного підходу, що поєднує різні методи та стратегії. Розробка та впровадження ефективних рішень у цій сфері вимагають глибокого розуміння потенційних загроз, а також знання про найкращі практики та інструменти для їх протидії. Нижче наведено ключові методи, які використовуються у сфері кібербезпеки для забезпечення захисту інформаційних систем та мереж від різноманітних кіберзагроз. Ці методи охоплюють широкий спектр дій, від ідентифікації та аналізу ризиків до реагування на інциденти та підвищення обізнаності серед персоналу:

1) Ідентифікація та аналіз ризиків охоплює ретельне вивчення існуючих та потенційних загроз безпеці інформаційних систем та використання інструментів для сканування мереж на предмет вразливостей;

2) Розробка та впровадження політик безпеки включає створення детальних політик безпеки, які регулюють використання інформаційних ресурсів, та проведення навчань для співробітників;

3) Захист інфраструктури вимагає встановлення комплексних систем безпеки та реалізації фізичних заходів для захисту обладнання;

4) Автоматизація безпеки та відповіді на інциденти передбачає використання автоматизованих систем для відповіді на загрози та розробку планів реагування на інциденти;

5) Навчання та підвищення обізнаності полягає у розробці та проведенні програм для підвищення обізнаності працівників про кіберзагрози.

6) Моніторинг та аналіз включають в себе застосування систем моніторингу для відстеження мережевого трафіку та аналіз великих даних для ідентифікації кіберзагроз;

7) Інтеграція та адаптація технологій вимагають створення єдиної системи захисту, що охоплює всі рівні інформаційних систем та постійне оновлення та модернізація інфраструктури безпеки.

2 МЕТОДИ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ АКТИВНИХ ДІЙ В КІБЕРБЕЗПЕЦІ

2.1 Опис інформаційних технологій та інструментів активних дій.

Інформаційні технології в кібербезпеці відіграють критично важливу роль у захисті цифрових систем та мереж від різноманітних кіберзагроз. Вони охоплюють широкий спектр інструментів, методів та практик, спрямованих на запобігання, виявлення, реагування та відновлення після кібератак. Інформаційні технології у цій галузі є особливо важливими, оскільки кіберзагрози стають все більш складними та розвинутими, вимагаючи від організацій більш вдосконалених та ефективних заходів безпеки.

Одним із ключових аспектів інформаційних технологій у кібербезпеці є використання систем виявлення вторгнень (IDS) та систем управління інцидентами безпеки (SIEM) [5]. IDS дозволяють ідентифікувати підозрілу активність у мережі, аналізуючи мережевий трафік і порівнюючи його з відомими патернами атак. SIEM системи інтегрують та аналізують дані безпеки з різних джерел, надаючи загальний огляд стану безпеки організації та дозволяючи швидко відповідати на будь-які інциденти.

Іншим важливим елементом є використання криптографії для захисту даних. Шифрування даних відіграє ключову роль у захисті конфіденційності та цілісності інформації, перешкоджаючи несанкціонованому доступу або змінам даних. Важливо, що сучасні криптографічні методи постійно розвиваються, щоб відповідати зростаючим вимогам безпеки та протидіяти новим методам кібератак.

Розвиток хмарних технологій також впливає на стратегії кібербезпеки. Хмарні сервіси пропонують гнучкість та масштабованість, але також створюють нові виклики для безпеки. Впровадження хмарних сервісів вимагає від організацій розробки нових стратегій та політик безпеки, адаптованих до хмарного середовища. Це включає контроль доступу, шифрування даних у хмарі та моніторинг хмарних ресурсів.

Зростання важливості мобільних пристроїв у бізнесі та особистому використанні також призвело до необхідності розширення кібербезпеки на ці пристрої. Мобільна безпека включає захист пристроїв від шкідливого програмного забезпечення, захист даних, що зберігаються та передаються з мобільних пристроїв, та управління доступом до корпоративних мереж.

Штучний інтелект (ШІ) та машинне навчання відкривають нові перспективи в кібербезпеці, дозволяючи системам аналізувати великі обсяги даних для виявлення складних шаблонів поведінки, що можуть вказувати на кібератаки. Ці технології дозволяють виявляти та відповідати на загрози швидше, ніж це можливо за допомогою традиційних методів.

Однак, кібербезпека не обмежується лише технологічними рішеннями. Важливою складовою є розробка та впровадження політик безпеки, підготовка та навчання персоналу, регулярні аудити та оцінки ризиків. Людський фактор часто є найбільш вразливою ланкою у безпеці, тому забезпечення обізнаності та підготовки співробітників є критично важливим для ефективної кібербезпеки.

У сукупності, інформаційні технології у кібербезпеці формують комплексну та багаторівневу систему захисту, що поєднує технологічні інновації, стратегічне планування та людський фактор. У цьому динамічному та постійно змінюваному середовищі, постійне оновлення знань, навичок та технологій є ключем до захисту від сучасних та майбутніх кіберзагроз [6].

Огляд доступних публікацій, методик та практичних розробок у галузі інформаційних технологій та інструментів активних дій у кібербезпеці відкриває перед нами комплексний світ сучасних стратегій та рішень, що використовуються для захисту від постійно зростаючих кіберзагроз. У цьому контексті, активні дії в кібербезпеці включають широкий спектр заходів, починаючи від моніторингу мережевої активності і закінчуючи розробкою комплексних систем виявлення та реагування на загрози.

Сучасні наукові дослідження у цій області часто зосереджені на використанні передових технологій, таких як штучний інтелект (ШІ), машинне навчання та аналітика великих даних. Ці технології дозволяють не лише

виявляти та аналізувати кіберзагрози в реальному часі, але й прогнозувати потенційні атаки, адаптуючись до нових методів ведення кібервійн.

Публікації у цій сфері також часто зосереджуються на розвитку та впровадженні політик безпеки, що включають стандартизацію процесів та процедур, регулярні аудити та оцінки ризиків. Значна увага приділяється також підготовці та навчанню персоналу, оскільки людський фактор залишається одним з найбільш вразливих аспектів у кібербезпеці.

Враховуючи швидкий розвиток кіберзагроз, багато досліджень акцентують на необхідності постійного оновлення та адаптації методів кібербезпеки. Це включає розробку адаптивних систем, здатних швидко реагувати на змінювані умови та нові види атак. Крім того, велика увага приділяється етичним аспектам використання інформаційних технологій у кібербезпеці, особливо з огляду на збільшення обсягу збору та аналізу даних.

З огляду на все вищесказане, можна зробити висновок, що сфера інформаційних технологій та інструментів активних дій у кібербезпеці знаходиться у стані постійного розвитку. Вона вимагає не лише технічних знань та навичок, але й глибокого розуміння потенційних кіберзагроз та стратегій їх протидії. У цьому контексті, важливим є не лише впровадження новітніх технологій, але й розробка комплексних стратегій безпеки, які враховують різноманітні аспекти цієї швидко змінюваної галузі.

2.2 Вибір методів рішення задачі

Ефективні програми систем виявлення та запобігання вторгнень (IDS/IPS) є ключовими компонентами сучасної інфраструктури кібербезпеки. Вони виконують життєво важливу роль у виявленні та нейтралізації кіберзагроз, забезпечуючи захист від несанкціонованого доступу, шкідливих атак та інших форм кіберзлочинності. Основна мета цих систем полягає у моніторингу мережевого трафіку та активності користувачів для ідентифікації підозрілих або ворожих дій, що можуть становити загрозу для мережевої інфраструктури.

Системи виявлення вторгнень (IDS) працюють шляхом моніторингу та аналізу мережевого трафіку та системних журналів на наявність підозрілої активності. IDS можуть бути розділені на дві основні категорії: мережеві IDS (NIDS), які аналізують мережевий трафік для виявлення підозрілих патернів поведінки, та хостові IDS [6] (HIDS), які зосереджені на моніторингу та аналізі активності на конкретному комп'ютері або сервері. IDS системи генерують сповіщення при виявленні потенційних загроз, дозволяючи IT-спеціалістам вживати відповідних заходів.

Системи запобігання вторгненням (IPS), з іншого боку, не тільки виявляють підозрілі дії, але й активно втручаються для блокування або запобігання цим діям. IPS системи часто інтегруються з мережевою інфраструктурою та автоматично реагують на виявлені загрози, блокуючи шкідливий трафік або відключаючи вразливі сервіси. Вони використовують різноманітні методи для виявлення та запобігання атакам, включаючи підписи загроз, аналіз аномалій та поведінкові методи.

Ефективність IDS/IPS систем значною мірою залежить від їх здатності точно виявляти реальні загрози, мінімізуючи при цьому помилкові спрацювання. Це вимагає регулярного оновлення баз даних підписів та алгоритмів, а також налаштування систем відповідно до специфічного мережевого середовища та політики безпеки організації.

2.2.1 Snort

Snort – це програма системи виявлення вторгнень в мережу з відкритим кодом, яка підтримується різними операційними системами. Система Snort була розроблена як самостійне програмне забезпечення та в 2008 році була придбана компанією Cisco, що нині виступає її партнером та розробником. Snort визнаний оптимальним рішенням для малих та середніх компаній. Утиліта включає сніфер пакетів, підтримує правила конфігурації та інші функції. Snort – ідеальний інструмент для тих, хто шукає зрозумілу та функціональну систему для запобігання вторгненням [6].

На рисунку 2.1 зображено логотип програми Snort.

Рисунок 2.1 – Логотип програми Snort

Snort оснащений можливістю ведення протоколів, аналізу та пошуку за змістом. Цей інструмент може використовуватися як для активного блокування, так і для пасивного виявлення широкого спектра атак і зондувань. Snort відзначається здатністю виявляти атаки, які проводяться під прикриттям, коли зловмисник відсилає безліч підозрілих пакетів на цільову систему.

Snort впроваджує прогресивний підхід до обробки пакетів. Кожен пакет, що потрапляє в Snort, проходить через послідовний ряд етапів, включаючи декодери та препроцесори, перш ніж надходить до детектора, який використовує правила для виявлення потенційних атак.

Snort працює наступним чином:

Пакет проходить через декодер, препроцесор, а потім у детектор, де детектор починає застосовувати правила. Завдання декодера полягає в тому, щоб витягти мережеві та транспортні дані (IP, TCP, UDP) із протоколів канального рівня. Завдання препроцесора — підготувати дані з протоколів транспортного рівня та мережевого рівня для процесу застосування правил.

Наприклад, ви можете використовувати препроцесор для обробки TCP, який зазвичай вирішує наступний список завдань [7]:

1) Контроль стану (контроль відповідності протоколу);
2) Збір сеансів (комбінація даних з кількох пакетів сеансів);
3) Стандартизація протоколу.

Правильне налаштування препроцесора може значно покращити продуктивність системи та зменшити кількість непотрібних даних, що надходять у детектор. Крім того, завдяки особливостям цієї архітектури до Snort відносно легко підключити власний препроцесор. В результаті перед відправкою в детектор формуються «надпакети», до яких починають застосовуватися правила. Процес застосування правил зводиться до пошуку в «надпакеті», визначених у правилі сигнатур. Самі правила складаються з опису трафіку, сигнатури, опису загрози та опису реакції на виявлення.

2.2.2 Wazuh

Wazuh вирізняється як потужний та високопродуктивний інструмент, розроблений для виявлення вторгнень, управління подіями та забезпечення високого рівня безпеки інформаційних систем.

Однією з ключових переваг Wazuh є його спроможність збирати, аналізувати та нормалізувати журнальні дані з різних джерел, надаючи повний обсяг інформації для моніторингу безпеки. Це реалізується за допомогою агентів Wazuh, які розгортаються на серверах та кінцевих точках, надаючи системі здатність аналізувати та реагувати в реальному часі.

Виявлення вторгнень є ключовим аспектом кібербезпеки, і Wazuh використовує різноманітні методи для цього. Застосування сигнатур, правил та алгоритмів машинного навчання дозволяє програмі ефективно розпізнавати аномалії та інші загрози безпеки. Інтеграція з базами даних загроз допомагає виявляти та блокувати відомі види атак.

Окрім виявлення вторгнень, Wazuh надає інтеграцію з системами управління інцидентами та подіями (SIEM), що сприяє ефективному управлінню інцидентами. Система аналізу та кореляції подій дозволяє з'єднувати інформацію з різних джерел, створюючи повніший контекст для аналізу інцидентів.

Важливим аспектом є також можливість адаптації Wazuh до конкретних потреб організації. Можливість власноруч налаштовувати правила та сигнатури дозволяє підлаштовувати програму під специфічні потреби та загрози.

Wazuh не лише надає надійний захист від кіберзагроз, але й забезпечує візуалізацію даних через інтеграцію з панеллю управління Kibana. Графіки, звіти та аналітика допомагають користувачам легше розуміти та відслідковувати стан безпеки.

У підсумку, Wazuh є важливим інструментом для будь-якої організації, що цінує ефективну кібербезпеку. Його розширюваність, гнучкість та здатність адаптації роблять його ідеальним вибором для підприємств будь-якого розміру, які прагнуть забезпечити захист своїх інформаційних ресурсів у сучасному цифровому середовищі.

На рисунку 2.2 зображено логотип програми Wazuh.

Рисунок 2.2 – Логотип програми Wazuh

2.2.3 Zenmap

Zenmap є графічним інтерфейсом для Nmap, одного з найвідоміших інструментів сканування мережі. Розроблений як відкритий додаток, Zenmap використовується кібербезпековими фахівцями, системними адміністраторами та тестувальниками на проникнення для картографування мережевої інфраструктури, аудиту безпеки та виявлення потенційних вразливостей.

На рисунку 2.3 зображено логотип програми Zenmap.

Рисунок 2.3 – Логотип програми Zenmap

Zenmap дозволяє користувачам визначати, які хости (комп'ютери та інші пристрої) активні у мережі, які порти відкриті на цих хостах, які програми слухають на цих портах, і які операційні системи вони використовують. Ця інформація є критично важливою для розуміння потенційних слабких місць у мережі, які можуть бути використані зловмисниками.

Робота Zenmap заснована на використанні різноманітних команд та скриптів Nmap, але з графічним інтерфейсом, що робить процес більш зручним та інтуїтивним, особливо для користувачів, які не звикли працювати з командним рядком. Інструмент може виконувати різні види сканувань, від простих пінгів до виявлення версій програмного забезпечення та операційних систем, а також виконання скриптів для автоматизації завдань сканування та аналізу.

Однією з ключових особливостей Zenmap є його здатність візуалізувати структуру мережі. Ця функція дозволяє користувачам бачити мережеву топологію в графічному форматі, що може бути надзвичайно корисним для розуміння взаємозв'язків між різними хостами та службами у мережі.

Завдяки своїй гнучкості та потужним можливостям, Zenmap широко використовується не лише для безпекових аудитів та виявлення вразливостей, але й для моніторингу мережевої інфраструктури, планування оновлень та вдосконалення мережевої архітектури. Його здатність адаптуватися до різних

сценаріїв робить його незамінним інструментом для будь-якого фахівця у сфері кібербезпеки.

2.2.4 Suricata

Suricata представляє собою потужний аналізатор мережевого трафіку з відкритим кодом, що використовується для виявлення вторгнень, моніторингу мережевого трафіку, а також забезпечення безпеки мережі. Цей інструмент розроблений для швидкого і глибокого аналізу мережевих даних, здатного виявляти складні загрози, які традиційні системи можуть пропустити.

На рисунку 2.4 зображено логотип програми Suricata.

Рисунок 2.4 – Логотип програми Suricata

Suricata розроблена з особливим акцентом на продуктивність і ефективність, забезпечуючи швидке оброблення великих обсягів мережевого трафіку, що є критично важливим для великих мережевих інфраструктур. Він може бути використаний як у великих організаціях, так і в невеликих мережах. Завдяки своїм високопродуктивним можливостям, Suricata ідеально підходить для моніторингу високошвидкісних мереж, де вона може аналізувати трафік в режимі реального часу без втрати продуктивності.

Однією з ключових особливостей Suricata є її здатність використовувати правила виявлення вторгнень для ідентифікації потенційних загроз. Ці правила можуть бути налаштовані та оновлені відповідно до змінюваних загроз, дозволяючи Suricata динамічно адаптуватися до нових викликів у кібербезпеці.

Крім того, Suricata підтримує багатопотокову обробку даних, що значно підвищує її продуктивність та забезпечує високу точність виявлення.

Suricata також підтримує глибокий аналіз пакетів (Deep Packet Inspection, DPI) [8], що дозволяє їй виявляти складні мережеві загрози, включаючи замасковані або зашифровані атаки. Завдяки цій можливості Suricata виявляє не тільки поверхневі атаки, а й складні маніпуляції з трафіком, що вимагають глибокого розуміння мережевих протоколів та патернів поведінки.

Використання Suricata як частини інтегрованої системи кібербезпеки може значно підвищити здатність організацій протистояти сучасним кіберзагрозам. Його гнучкість та сумісність з іншими інструментами безпеки, такими як файрволи та системи управління інцидентами, роблять його цінним доповненням до будь-якої стратегії кібербезпеки.

У підсумку, Suricata являє собою передовий інструмент для аналізу мережевого трафіку, який надає фахівцям з кібербезпеки можливість ефективно виявляти, аналізувати та реагувати на різноманітні кіберзагрози, тим самим забезпечуючи комплексний захист мережевих ресурсів.

2.2.5 McAfee Network Security Platform

McAfee Network Security Platform найкраще підходить для великих компаній, які можуть виділити великий бюджет на захист своїх мереж, оскільки продукт починається від 10 000 доларів США. Ціна прийнятна, оскільки цей IDS може блокувати велику кількість загроз, отримувати доступ до шкідливих сайтів, запобігати DDoS-атакам тощо.

На рисунку 2.5 зображено логотип програми McAfee Network Security Platform.

Рисунок 2.5 – Логотип програми McAfee Network Security Platform

Це рішення дозволяє блокувати нові та невідомі атаки шляхом перевірки трафіку з підписами та без них. Технологія безсигнатурного виявлення вторгнень дозволяє ідентифікувати зловмисний мережевий трафік і блокувати раніше невідомі атаки, де сигнатур не існує.

Підтримка McAfee Threat Intelligence Exchange дозволяє аналізувати загрози в реальному часі у фізичних і віртуальних мережах. Інтеграція з McAfee Advanced Threat Defense і McAfee MOVE AntiVirus, компонентами рішення McAfee Cloud Workload Security, дозволяє організаціям автоматизувати складні процеси безпеки в програмно-визначеному центрі обробки даних.

Ключові особливості цього програмного рішення такі [9]:

1) SSL-дешифрування для перевірки вхідного та вихідного мережевого трафіку;

2) Централізоване управління для оптимізації збору та контролю інформації;

3) Інтеграція з пакетом рішень McAfee для забезпечення повного захисту від пристрою до хмари.

2.2.6 Zeek

Zeek, раніше відомий як Bro, є потужним аналізатором мережевого трафіку з відкритим кодом, який широко використовується в галузі кібербезпеки. Ця система є унікальною через свою здатність не просто збирати дані про мережевий трафік, але й проводити глибокий аналіз цього трафіку, що дозволяє виявляти складні патерни поведінки та потенційні кіберзагрози.

На рисунку 2.6 зображено логотип програми Zeek.

Рисунок 2.6 – Логотип програми Zeek

Однією з ключових особливостей Zeek є його висока гнучкість. Він не обмежується лише виявленням відомих підписів атак, як традиційні системи виявлення вторгнень (IDS), але також здатен аналізувати мережевий трафік на більш високому рівні, ідентифікуючи аномалії, які можуть вказувати на зловмисні дії. Це робить Zeek винятково корисним у виявленні складних загроз, таких як нульові дні, складні персоналізовані атаки та інші тактики, які можуть уникнути виявлення традиційними IDS [10].

Zeek використовує потужний скриптовий мову, що дозволяє користувачам налаштовувати його поведінку та розширювати його функціональність. Ця мова скриптів дозволяє аналітикам кібербезпеки розробляти власні скрипти для обробки та аналізу мережевих даних, враховуючи конкретні потреби їхньої організації або дослідження. Такий підхід надає користувачам небачену досі гнучкість у моніторингу та аналізі мережевої активності.

Крім забезпечення безпеки, Zeek також використовується для мережевої діагностики та управління продуктивністю. Його здатність збирати детальні метадані про мережевий трафік робить його цінним інструментом для розуміння мережевої активності та виявлення потенційних проблем з продуктивністю або конфігурацією мережі.

У світі, де кіберзагрози стають все більш розумними та витонченими, інструменти як Zeek стають незамінними. Його здатність адаптуватися до

постійно змінюваних умов кіберпростору, виявляючи не тільки відомі атаки, але й нові, невідомі загрози, робить його ключовим компонентом в стратегіях кібербезпеки багатьох організацій. Zeek допомагає не лише виявляти та реагувати на атаки, але й сприяє глибшому розумінню загроз, що дозволяє спеціалістам кібербезпеки розробляти більш ефективні захисні стратегії.

2.3 Порівняльний аналіз IPS/IDS систем та виявлення їх недоліків

Snort вже давно є лідером у системах запобігання та виявлення вторгнень. Однак із розвитком нових технологій, появою багатоядерних процесорів, IPv6, збільшенням кількості користувальницьких додатків і зростанням трафіку ця система вже не може повністю адаптуватися до нових умов. Snort підтримує IPv6, може перевіряти додатки та багато іншого, але він все ще однопотоковий, що значно сповільнює його роботу. Альтернативою Snort є Suricata. Основна відмінність між цими двома інструментами полягає в тому, що Suricata багатопотоковий. Це означає, що інструмент може використовувати кілька ядер одночасно, що дозволяє краще балансувати навантаження.

Це дозволяє нам обробляти більше даних без необхідності повертатися до кількості запроваджених нами правил, що дає Suricata невелику перевагу над Snort.

Suricata формує вихід подій у форматі JSON, що значно спрощує інтеграцію Suricata зі сторонніми програмами, включаючи системи моніторингу та візуалізації журналів (наприклад, Kibana).

Однією з сильних сторін Suricata є його обробка OSI Layer 7, яка покращує його здатність виявляти зловмисне програмне забезпечення. У правилах не можна суворо прив'язувати номер порту, як це робиться в Snort, достатньо вказати протокол і операцію. Крім того, сам модуль Suricata буде обробляти трафік і виявляти протоколи, навіть якщо використовуються нестандартні порти [11].

Недоліками Suricata є велика кількість налаштувань і нечіткість деяких питань з документацією.

Zeek — чудовий інструмент для виявлення загроз. Багато IDS, наприклад Suricata, зосереджені на виявленні на основі підписів і правил. Zeek можна використовувати як традиційний IDS. Однак Zeek можна використовувати, щоб зосередитися на конкретних мережевих протоколах для глибшого аналізу. Чим більше даних вам доведеться обробити під час пошуку загроз, тим краще. Недоліком Zeek є складність спілкування з інструментом, оскільки технологія фокусується на функціональності, а не на графічних інтерфейсах [12].

McAfee Network Security Platform є досить дорогим рішенням, що є недоліком порівняно з іншими системами з відкритим кодом. Однак ця система більш ефективна в ситуаціях, коли потрібен максимальний захист мережі. Перевагою McAfee є те, що він працює як із сигнатурами, так і без них, що дозволяє виявляти раніше невідомі атаки. Іншим недоліком єуповільнення швидкості мережі через величезний обсяг функцій.

В таблиці 2.1 представлена порівняльна характеристика додатків.

Таблиця 2. 1 – Порівняльна характеристика додатків

Назва системи	**Переваги**	**Недоліки**	**Спосіб вирішення**
Snort	Здатність Snort виявляти та блокувати широкий спектр атак, навіть тих, що здійснюються під прикриттям, є ключовою перевагою цієї системи. Це забезпечує ефективний захист в широкому діапазоні кіберзагроз.	Однак Snort може уповільнити роботу через свою однопотоковість і обмеженість скануванням за певними номерами портів.	Модернізація системи, в тому числі оптимізація використання ресурсів і реалізація багатопотоковості, може покращити продуктивність.
Suricata	Система Suricata пропонує багатопотоковість та високу продуктивність, що полегшує інтеграцію зі сторонніми програмами та обробку даних на 7-му рівні OSI.	Складність налаштувань та в деяких випадках недостатньо чітка документація можуть стати перешкодою для користувачів.	Використання сторонніх програм, таких як Kibana, може полегшити взаємодію з системою.

Назва системи	Переваги	Недоліки	Спосіб вирішення
McAfee Network Security Platform	McAfee Network Security Platform надає можливість виявлення невідомих раніше атак та забезпечує високий рівень захисту мережі завдяки роботі як з сигнатурами, так і без них.	Висока вартість та потенційне уповільнення мережі через об'ємний функціонал.	Ця система оптимальна для сценаріїв, де виправдана потреба у максимальному захисті, незважаючи на високу вартість та можливе уповільнення мережі.
Zeek	Zeek підтримує різні режими роботи, забезпечуючи гнучкість через можливість користувацьких налаштувань і створення власних скриптів для політик та спеціалізованих аналізаторів протоколів.	Однак складність інтерфейсу та налаштувань може бути бар'єром для користувачів без великого досвіду в кібербезпеці.	Zeek найкраще підходить для використання досвідченими фахівцями у мережах, де необхідна велика гнучкість та детальні налаштування.

2.4 Розгляд конкретних кейсів використання інформаційних технологій та інструментів.

Аналіз конкретних кейсів використання інформаційних технологій та інструментів у кібербезпеці відкриває перед нами панораму реальних сценаріїв, в яких сучасні технології та стратегії застосовуються для захисту від кіберзагроз. В цьому контексті, кожен кейс використання демонструє, яким чином інструменти та методики можуть бути адаптовані до специфічних вимог і обставин, що виникають у реальному світі кібербезпеки [15] .

Один із найбільш інформативних прикладів застосування активних інструментів кібербезпеки включає використання систем виявлення вторгнень (IDS) і систем управління інцидентами безпеки (SIEM). Ці системи інтегруються в мережеву інфраструктуру та аналізують мережевий трафік, щоб виявити підозрілі або аномальні шаблони, які можуть вказувати на потенційну кібератаку. Наприклад, у випадку з фінансовими установами, де безпека даних має критичне значення, такі системи можуть виявляти спроби фішингу, розповсюдження шкідливого програмного забезпечення або спроби несанкціонованого доступу.

Іншим важливим аспектом є застосування штучного інтелекту та машинного навчання в кібербезпеці. Ці технології дозволяють системам кібербезпеки "навчатися" з попереднього досвіду та покращувати свою здатність виявляти та реагувати на нові види загроз. Наприклад, в області електронної комерції ці системи можуть аналізувати патерни покупців та виявляти потенційно шахрайські транзакції, запобігаючи фінансовим втратам та зловживанням даними.

Крім того, розвиток хмарних технологій відкрив нові можливості для кібербезпеки, особливо в плані масштабованості та гнучкості. Хмарні сервіси забезпечують можливість швидкого розгортання безпекових рішень, що є важливим для компаній, що працюють у динамічних умовах. Наприклад, під час раптового зростання трафіку або пікових навантажень, хмарні рішення дозволяють оперативно масштабувати захисні системи, не втрачаючи в продуктивності.

Також важливим є використання криптографічних методів для захисту даних. Шифрування даних є стандартною практикою для захисту конфіденційної інформації. В сучасному світі, де дані часто передаються через незахищені мережі, використання сильних криптографічних алгоритмів стає критично важливим для забезпечення конфіденційності та цілісності інформації.

Усі ці приклади відображають різноманітність підходів та стратегій в галузі кібербезпеки. Від моніторингу та виявлення до шифрування даних та використання хмарних технологій, кібербезпека вимагає комплексного підходу, що враховує специфіку діяльності організації, а також постійно розвивається ландшафт кіберзагроз. Використання цих технологій та методів у реальних сценаріях демонструє їхню ефективність та важливість для забезпечення безпеки в цифровому світі [17-19].

2.5 Технології та програмне забезпечення активних дій у кібербезпеці

Технології та програмне забезпечення, які використовуються для виконання активних дій у кібербезпеці, являють собою комплексний набір інструментів та систем, спрямованих на ідентифікацію, відслідковування, аналіз та протидію кіберзагрозам в реальному часі. Вони дозволяють організаціям не лише пасивно захищати свої мережі та системи, але й активно виявляти та реагувати на загрози, забезпечуючи таким чином більш високий рівень безпеки [20]:

1) Системи виявлення та попередження вторгнень (IDS/IPS) забезпечують моніторинг та аналіз мережевого трафіку для ідентифікації потенційно несанкціонованого доступу, а також активно блокують атаки за виявленими ознаками;

2) Штучний інтелект (ШІ) та машинне навчання використовуються для аналізу великих даних та виявлення складних шаблонів поведінки, а також для автоматизації відповіді на загрози;

3) Системи управління інцидентами безпеки (SIEM) збирають та аналізують безпекові дані для відстеження та аналізу інцидентів, забезпечуючи комплексне управління безпекою;

4) Хмарні рішення та безпека пропонують гнучкі та масштабовані безпекові рішення, що дозволяють централізувати управління безпекою та покращити моніторинг;

5) Аналітика великих даних дозволяє ідентифікувати складні загрози та поведінкові шаблони, покращуючи здатність організацій реагувати на кіберзагрози;

6) Кіберрозвідка та протидія включають збір інформації про потенційних загрозах та розробку стратегій протидії, щоб адаптувати та вдосконалити загальну стратегію безпеки.

Застосування цих технологій та програмного забезпечення в кібербезпеці дозволяє організаціям не лише реагувати на існуючі загрози, але й прогнозувати майбутні атаки, адаптуватися до постійно змінюваного ландшафту кіберзагроз та вдосконалювати свої стратегії захисту. Використання сучасних інформаційних технологій у кібербезпеці є ключовим для захисту від складних та розвинутих загроз, які постійно еволюціонують у сучасному цифровому світі [21-22].

3 ПРАКТИЧНА ЧАСТИНА

3.1 Приклади успішного використання інструментів в реальних випадках.

У сфері кібербезпеки реальні приклади ефективного використання інструментів є різноманітними та повчальними.

Одним з прикладів є велика фінансова установа, яка одного разу зіткнулася з постійними загрозами від фішингових атак. Вони впровадили вдосконалену систему фільтрації електронної пошти, яка використовувала машинне навчання для розпізнавання та карантинування фішингових електронних листів. Ця система постійно навчалася на нових даних, що значно підвищило рівень її виявлення і значно зменшило кількість успішних фішингових атак.

Інший випадок стосувався державної установи, яка стала мішенню серії розподілених атак на відмову в обслуговуванні (DDoS). В результаті було розгорнуто інтелектуальну службу пом'якшення наслідків DDoS-атак, яка могла розрізняти зловмисний і легальний трафік. Ця служба використовувала поведінковий аналіз для розуміння нормальних моделей трафіку та виявлення аномалій. В результаті агентство змогло підтримувати свої онлайн-сервіси безперебійно, незважаючи на постійні спроби атак.

Крім того, технологічна компанія, що працює з чутливою інтелектуальною власністю, використала комбінацію систем виявлення вторгнень (IDS) і систем запобігання вторгненням (IPS) для захисту своєї мережі. IDS відстежувала мережевий трафік на наявність ознак вторгнення, а IPS вживала негайних заходів для блокування зловмисної активності. Така проактивна позиція дозволила їм запобігти сучасній постійній загрозі (APT), яка була розроблена для крадіжки комерційної таємниці.

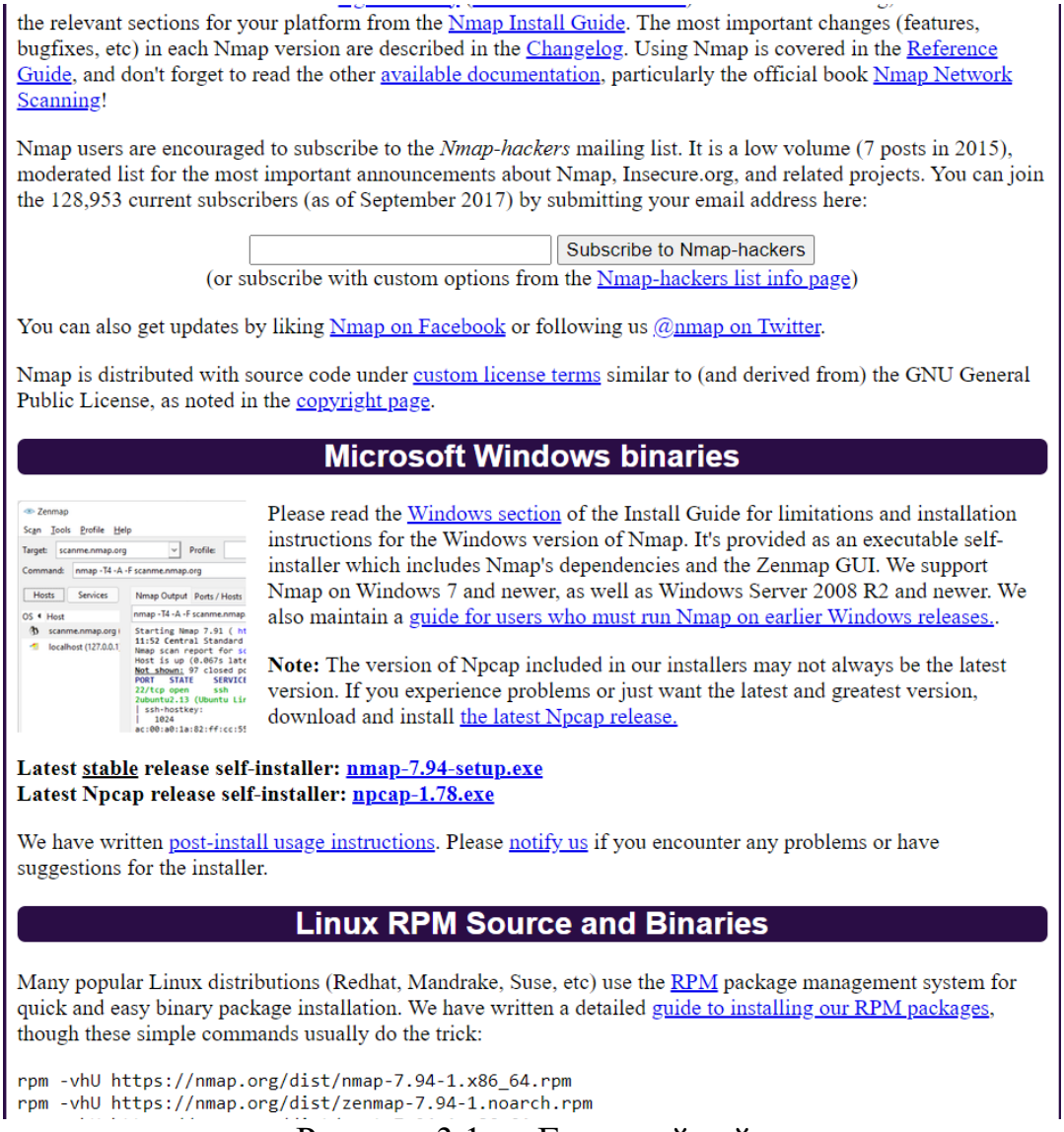
Ці приклади ілюструють важливість вибору правильних інструментів для конкретних потреб безпеки і силу адаптивних, інтелектуальних систем у захисті від складних кіберзагроз. Успіх цих інструментів залежить не лише від

їхньої технологічної досконалості, але й від їхньої правильної конфігурації, регулярного оновлення та інтеграції в комплексну стратегію безпеки.

3.2 Застосування програмного продукту Zenmap

Zenmap є графічним інтерфейсом для Nmap, одного з найвідоміших інструментів сканування мережі. Розроблений як відкритий додаток, Zenmap використовується фахівцями з кібербезпеки, системними адміністраторами та тестувальниками на проникнення для картографування мережевої інфраструктури, аудиту безпеки та виявлення потенційних вразливостей.

Для початку роботи програми її потрібно завантажити та інсталювати з офіційного сайту, де є дві версії з графічним інтерфейсом (Zenmap) та в командному рядку (Nmap) (рис.3.1).


the relevant sections for your platform from the Nmap Install Guide. The most important changes (features, bugfixes, etc) in each Nmap version are described in the Changelog. Using Nmap is covered in the Reference Guide, and don't forget to read the other available documentation, particularly the official book Nmap Network Scanning!

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

Subscribe to Nmap-hackers

(or subscribe with custom options from the Nmap-hackers list info page)

You can also get updates by liking Nmap on Facebook or following us @nmap on Twitter.

Nmap is distributed with source code under custom license terms similar to (and derived from) the GNU General Public License, as noted in the copyright page.

Microsoft Windows binaries

Please read the Windows section of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-installer which includes Nmap's dependencies and the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a guide for users who must run Nmap on earlier Windows releases..

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install the latest Npcap release.

Latest stable release self-installer: nmap-7.94-setup.exe
Latest Npcap release self-installer: npcap-1.78.exe

We have written post-install usage instructions. Please notify us if you encounter any problems or have suggestions for the installer.

Linux RPM Source and Binaries

Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the RPM package management system for quick and easy binary package installation. We have written a detailed guide to installing our RPM packages, though these simple commands usually do the trick:

```
rpm -vhU https://nmap.org/dist/nmap-7.94-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.94-1.noarch.rpm
```

Рисунок 3.1 – Головний сайт

Після завантаження інсталяційного пакету необхідно обрати необхідні компоненти та інсталювати додаток (рис.3.2).

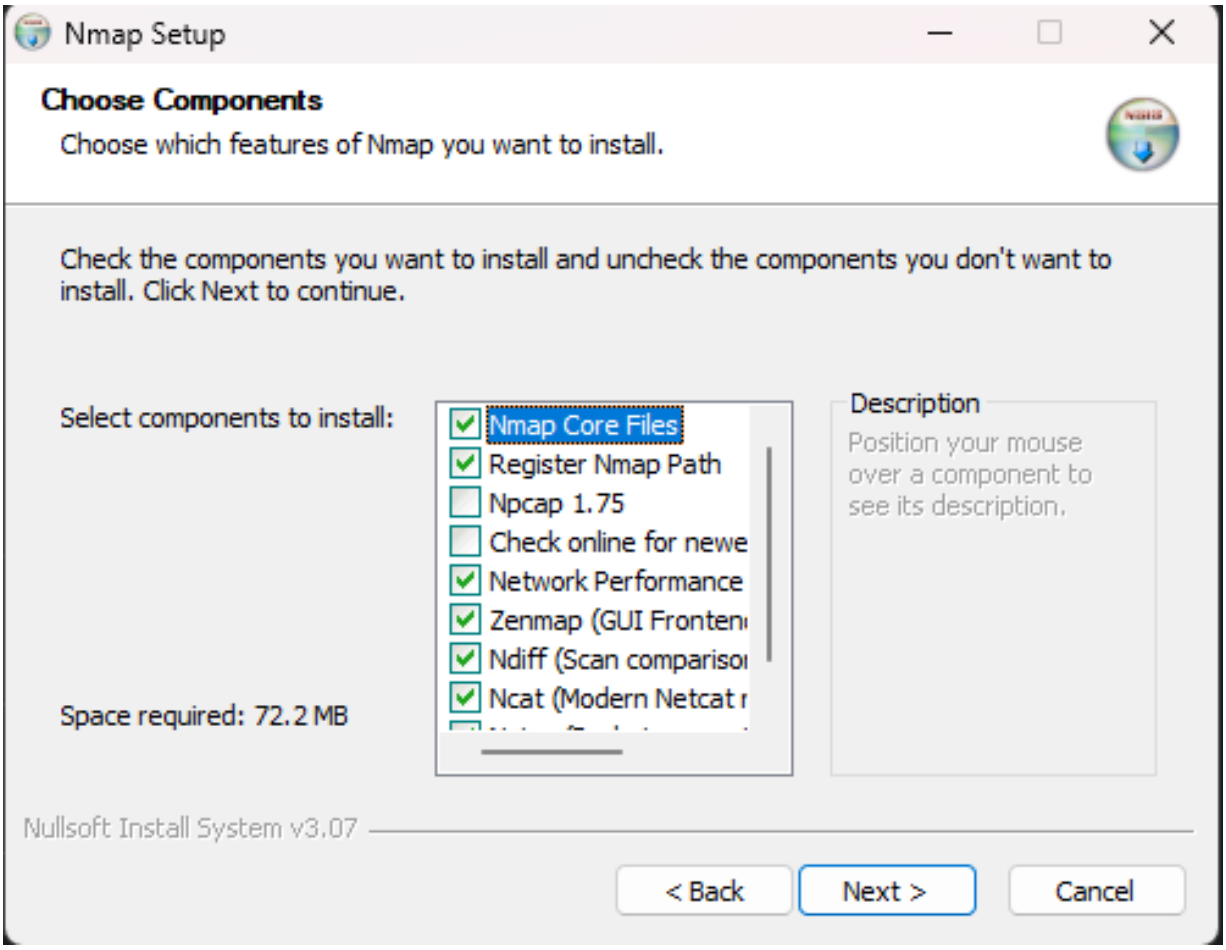


Рисунок 3.2 – Інсталяція додатку Zenmap

Програма має простий та зрозумілий інтерфейс. Після інсталяції Zenmap автоматично запускається та готова до початку роботи та сканування мережі (рис. 3.3).

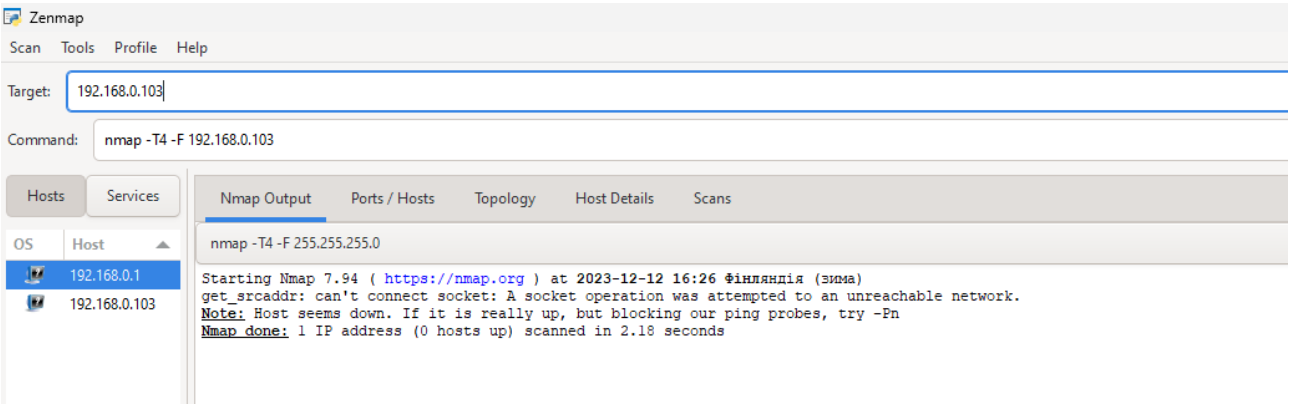


Рисунок 3.3 – Zenmap

Zenmap має наступні види сканувань:

1. Інтенсивне сканування: Виконує швидке сканування найбільш поширених TCP портів, намагаючись визначити тип ОС і які служби та їх версії працюють;

2. Інтенсивне сканування + UDP: Подібне до звичайного інтенсивного сканування, але включає також сканування UDP портів;

3. Інтенсивне сканування всіх TCP портів: Сканує всі TCP порти від 1 до 65535, не залишаючи жодного порту без уваги;

4. Інтенсивне сканування без пінга: Припускає, що запитуваний хост доступний та корисна, якщо ціль блокує запити пінгу;

5. Пінг-сканування: Виконує лише пінг цільових хостів, не включаючи сканування портів;

6. Швидке сканування: Швидше за інтенсивне сканування, обмежується лише топ-100 найпоширенішими TCP-портами;

7. Швидке сканування плюс: Додає невелике визначення версій та ОС до швидкого сканування;

8. Швидкий трасувальний маршрут: Використовується для визначення хостів і маршрутизаторів у мережевому скануванні;

9. Регулярне сканування: Використовує стандартні налаштування, виконуючи TCP SYN сканування для 1000 найпоширеніших TCP портів;

10. Повільне ретельне сканування: Включає ряд додаткових опцій для визначення хостів та ОС, використовуючи TCP, UDP, та інші протоколи/

Кожен тип сканування в Zenmap має свої специфічні цілі та використовується для різних сценаріїв, дозволяючи отримати детальну інформацію про мережеву інфраструктуру та потенційні вразливості.

На рисунку 3.4 представлено результати сканування мережі.

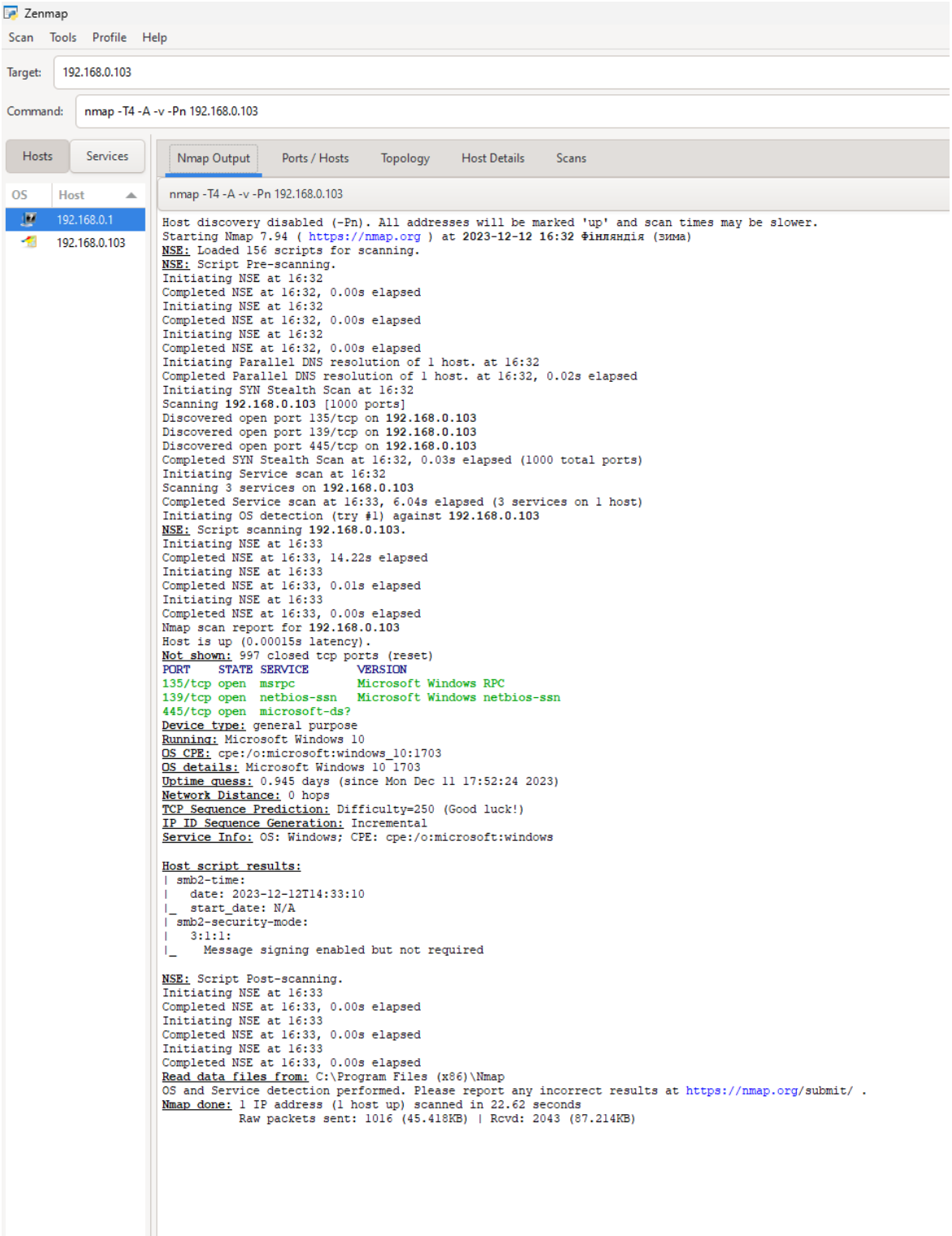


Рисунок 3.4 – Вивід результатів сканування

Вивід результатів сканування показує стандартні дані zenmap порти і хости показує порти протоколи стан виявлених портів і служби які працюють.

Також в даному додатку доступний вивід топології мережі в графічному режимі (рис. 3.5).

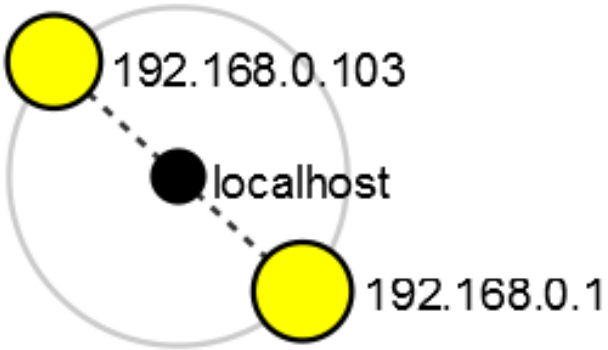


Рисунок 3.5 – Топологія в графічному режимі

На виявлених портах показано топологію мережі в графічному режимі. Топологію можна збільшувати та зменшувати, а також зберігати у вигляді зображення.

Деталі хоста показують інформацію про виявлені хости, які включають в себе ім'я хостів, їх стан, час їх роботи без перезавантаження та збоїв та багато іншого (рис. 3.6 та 3.7).

Сканування відображає історію всіх виконаних перевірок включно з запущеними перевірками.

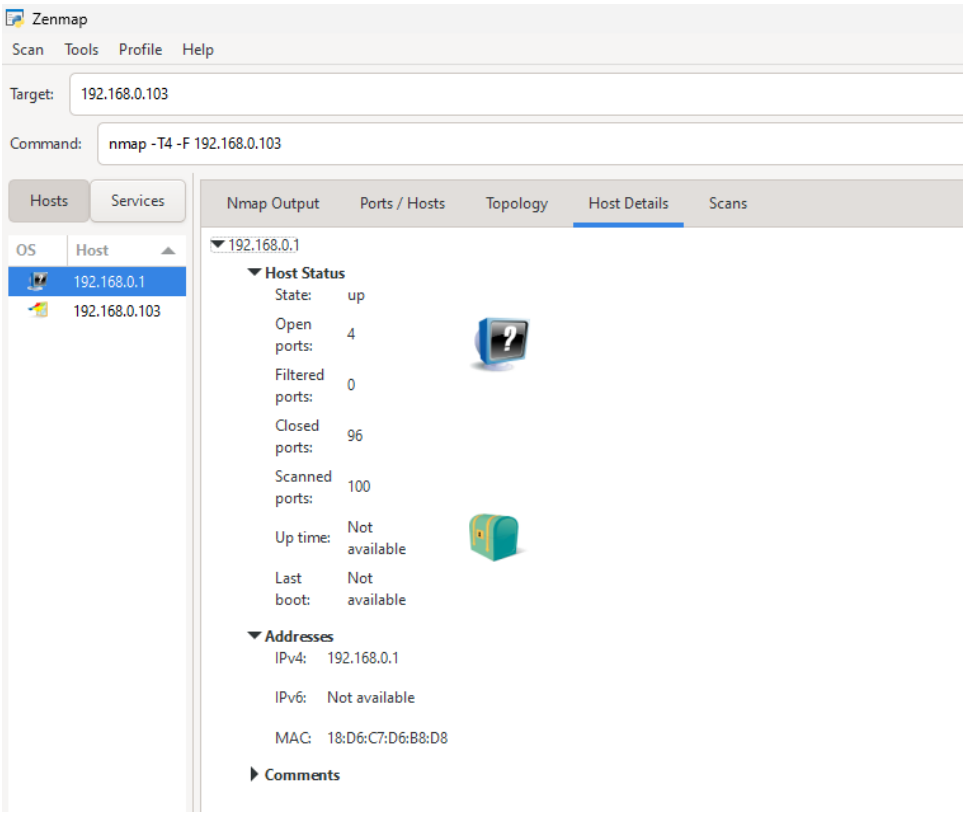


Рисунок 3.6 – Деталі хоста

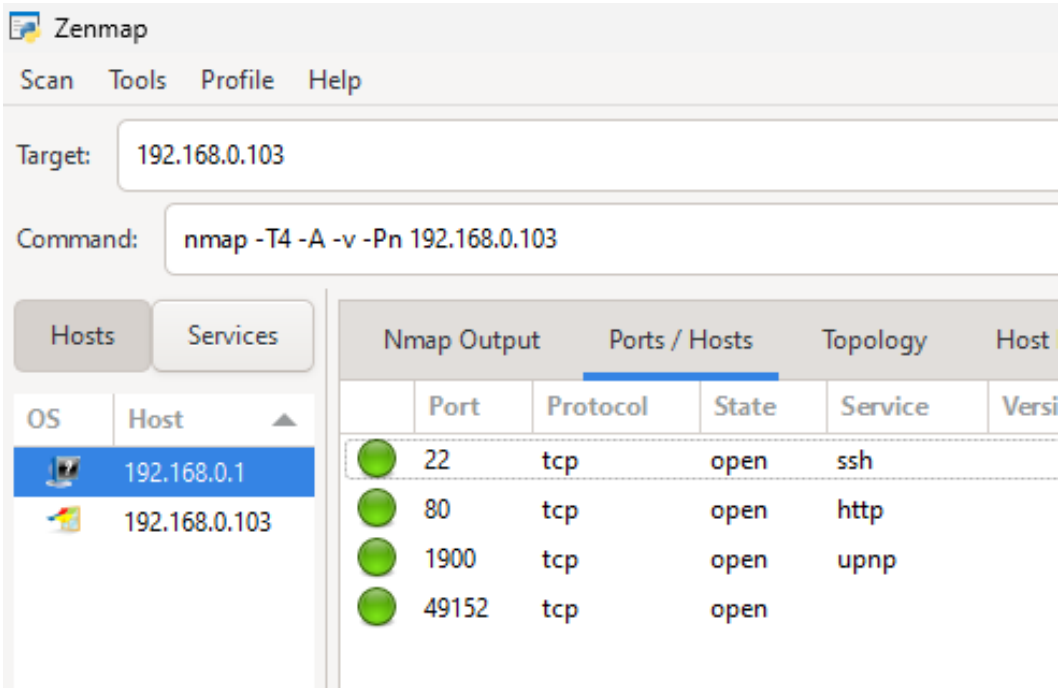


Рисунок 3.7 – Порти та хости

Також в zenmap є можливість створювати, редагувати та зберігати профілі сканування самостійно. Для цього потрібно:

1) перейти на вкладку «Профіль»;
2) натиснути «Новий профіль або команда»;
3) налаштувати необхідні параметри сканування і зберегти профіль .

Після цього він з'явиться на вкладці «Профілі сканування» (рис. 3.8 та 3.9).

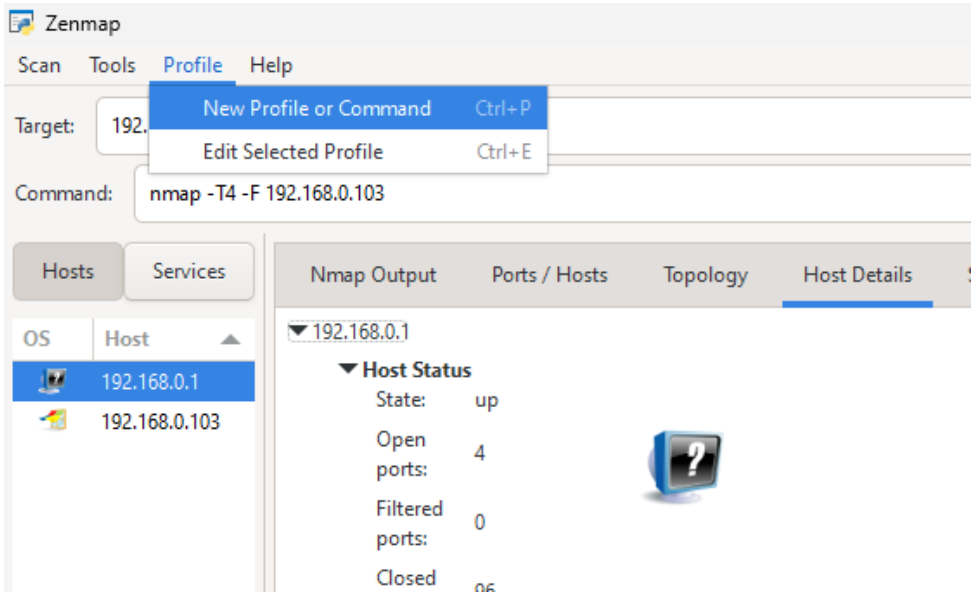


Рисунок 3.8 – Налаштування параметрів власного сканування

Процес створення власного сканування не займає більше декількох хвилин, навіть для недосвідчених користувачів. Потрібно вести IP-адресу для подальшого сканування.

Під час створення власних сканувань у Zenmap важливо розуміти різні параметри та опції, які пропонує Nmap, оскільки це дасть більшу гнучкість та контроль над процесом сканування. Також важливо враховувати етичні та правові аспекти сканування мереж, оскільки сканування чужих мереж без дозволу може бути незаконним.

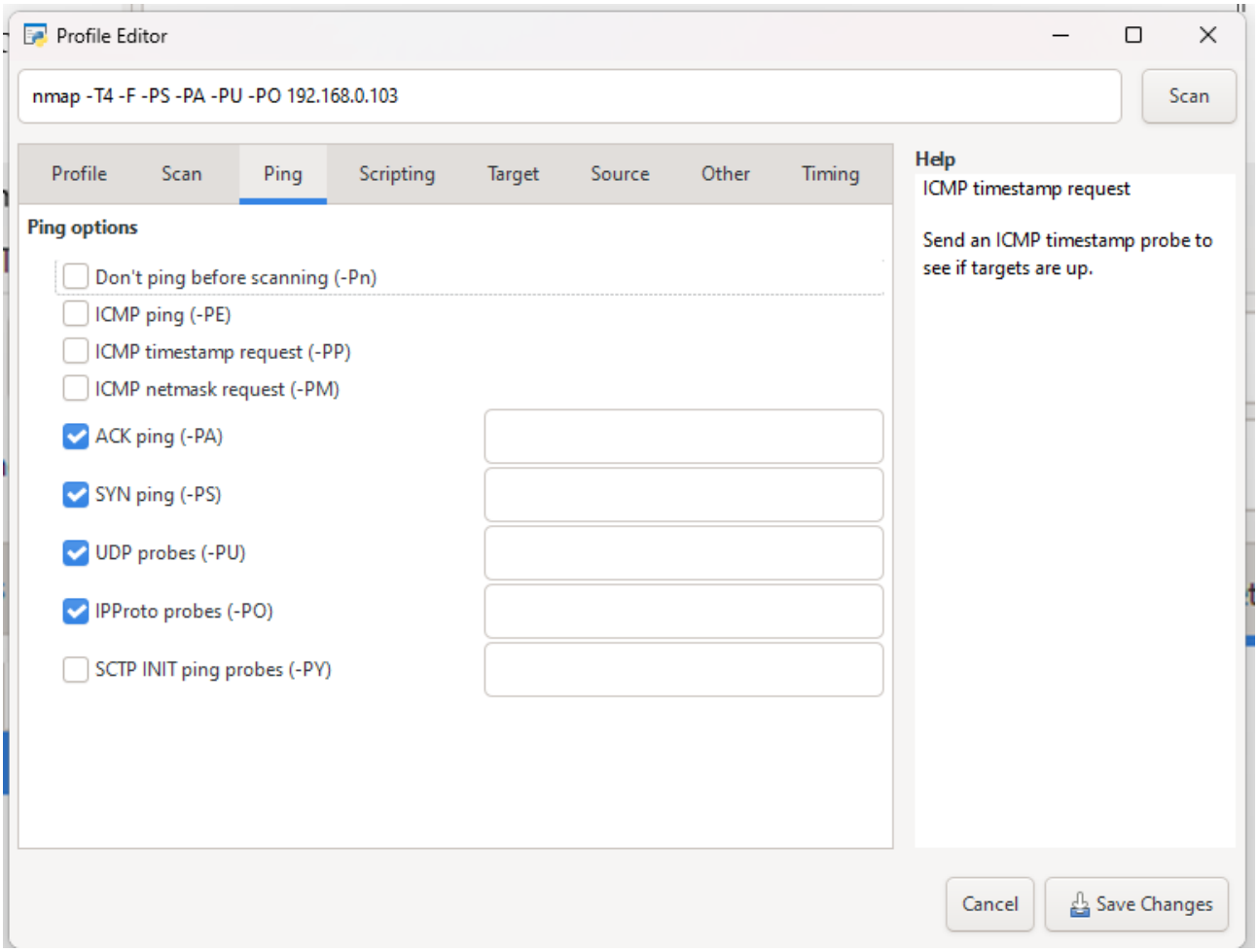


Рисунок 3.9 – Створення кастомного сканування

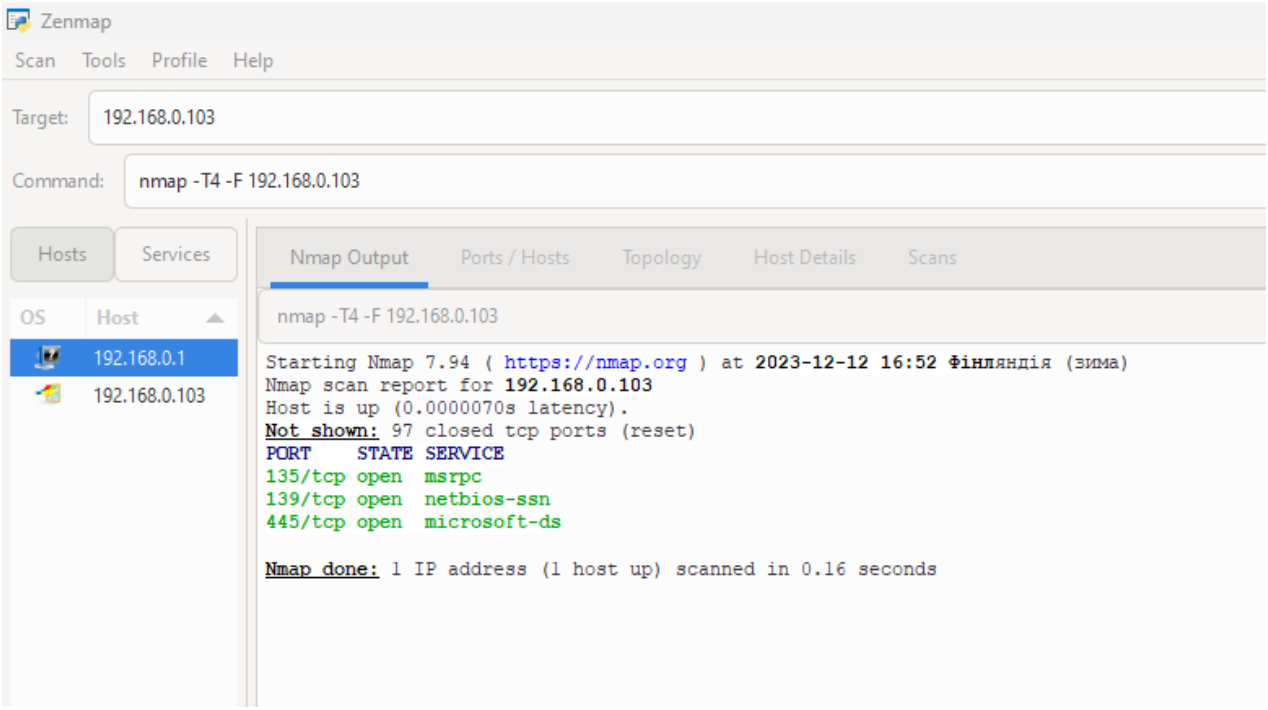


Рисунок 3.11 – Власне сканування

3.3 Застосування програмного продукту Wazuh

Моніторинг за допомогою Wazuh: На рис.3.12 відображається інформаційна панель Wazuh, яка надає візуальне резюме подій безпеки. Wazuh агрегує дані з різних джерел, щоб представити сповіщення про загрози в реальному часі. До неї підключено 3 користувачі, а саме власний ПК, на якому можна спостерігати роботу Wazuh, та 2 віртуальні машини на базі операційної системи Ubuntu, які будуть емулювати роботу як сайту, на який буде проведена атака, так і користувача який її буде створювати.

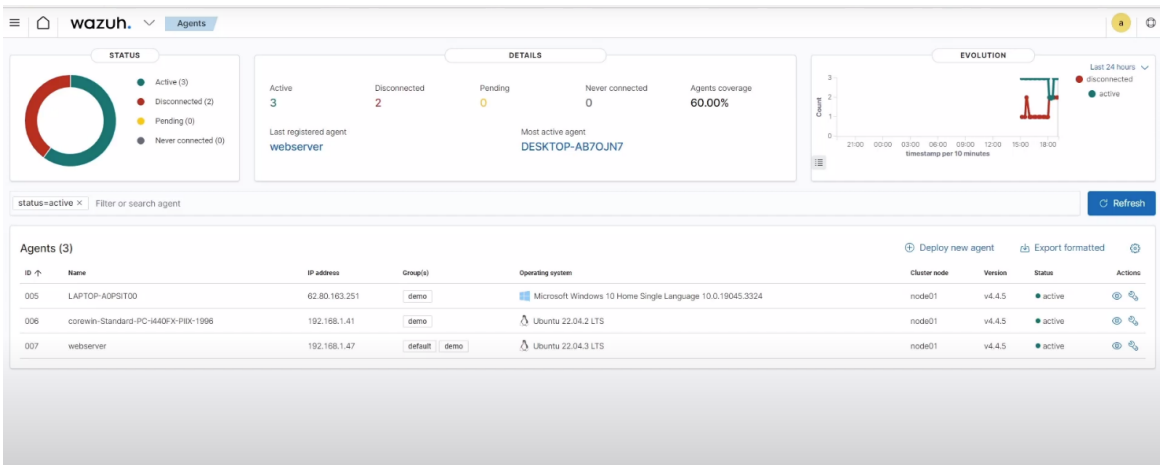


Рисунок 3.12 – Моніторинг Wazuh

Далі іде підключення по SSH для подальших дій та запуску серверу. На рис. 3.13 показано з'єднання з комп'ютером за допомогою Secure Shell (SSH) - протоколу для безпечного доступу до мережевих служб через незахищену мережу.

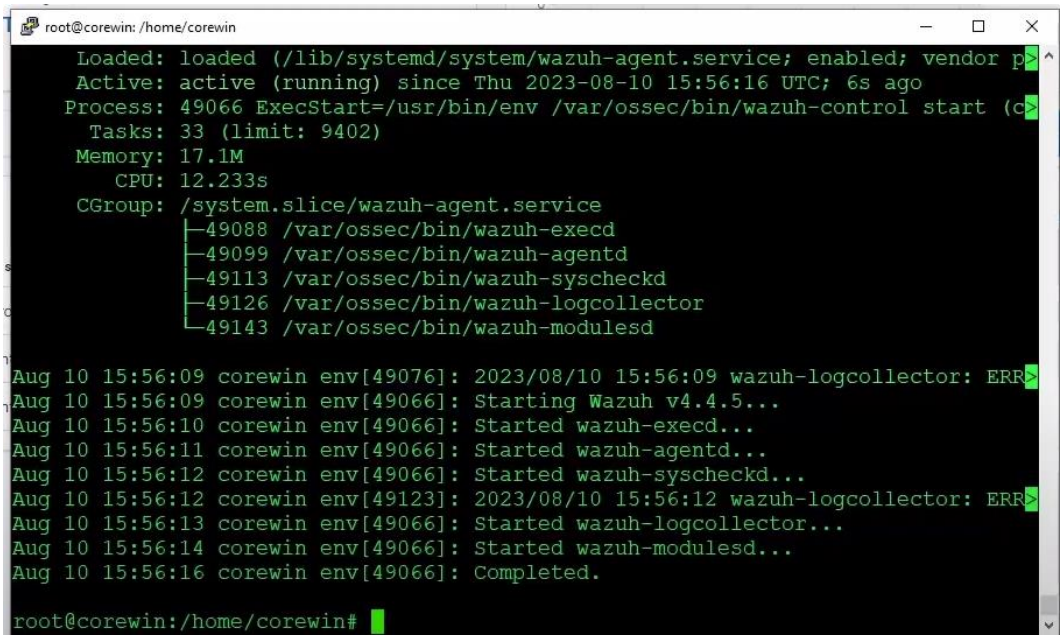


Рисунок 3.13 – Підключення по SSH

Після вдалого підключення потрібно запустити сервер Apache. На рис.3.14 зображено процес запуску сервера Apache та перевірки його статусу на коректну роботу, підкреслюючи готовність системи до обслуговування веб-сторінок або додатків.

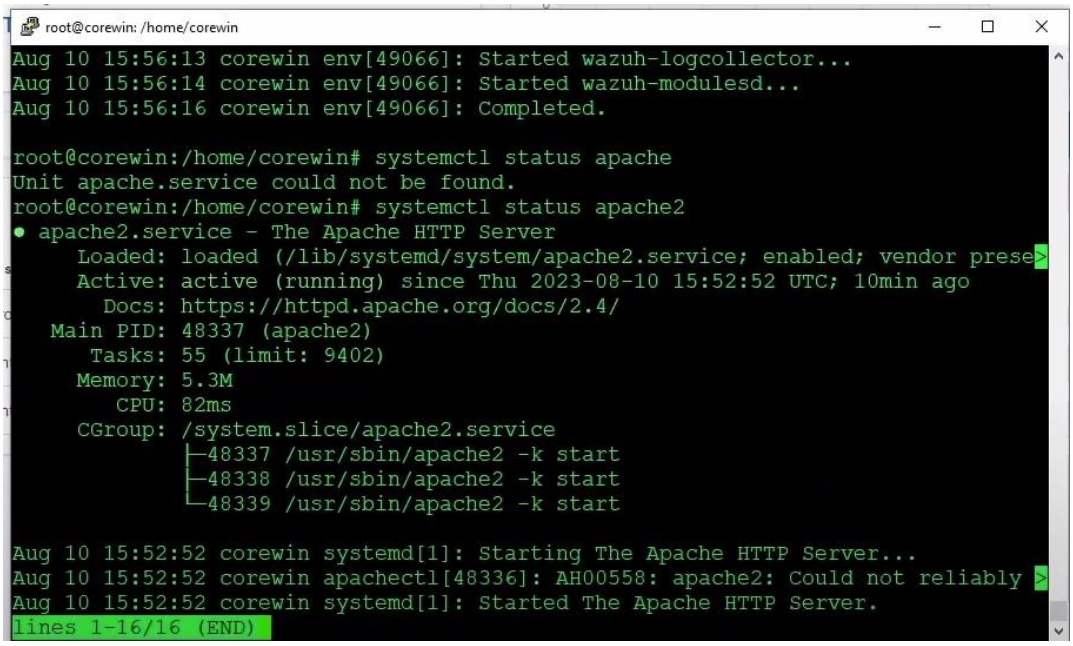


Рисунок 3.14 – Процес запуску сервера

Після перевірки на коректність роботи потрібно відкрити налаштування на конкретній віртуальній машині (рис.3.15).

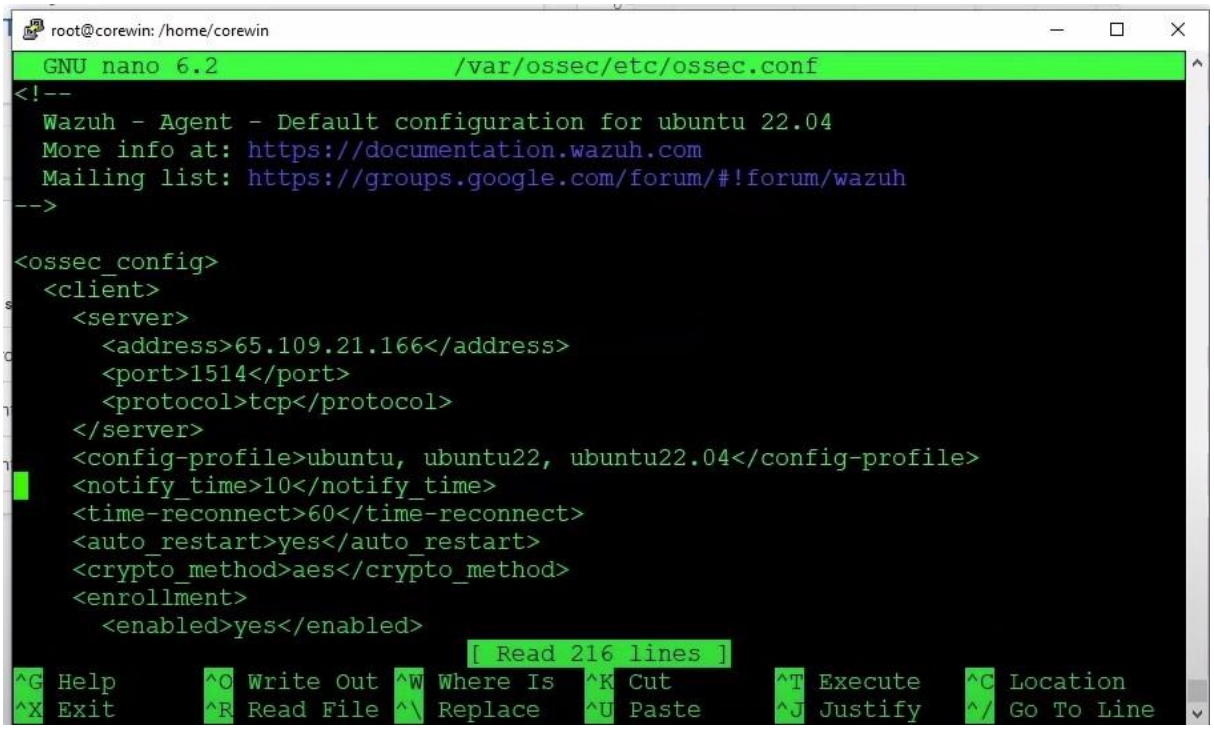


Рисунок 3.15 – Налаштування на віртуальній машині

В самому файлі з налаштуваннями потрібно додати секцію котра буде відповідати за моніторинг файлів, вона має вигляд <localfile> та додається формат та місце знаходження логу (рис.3.16).

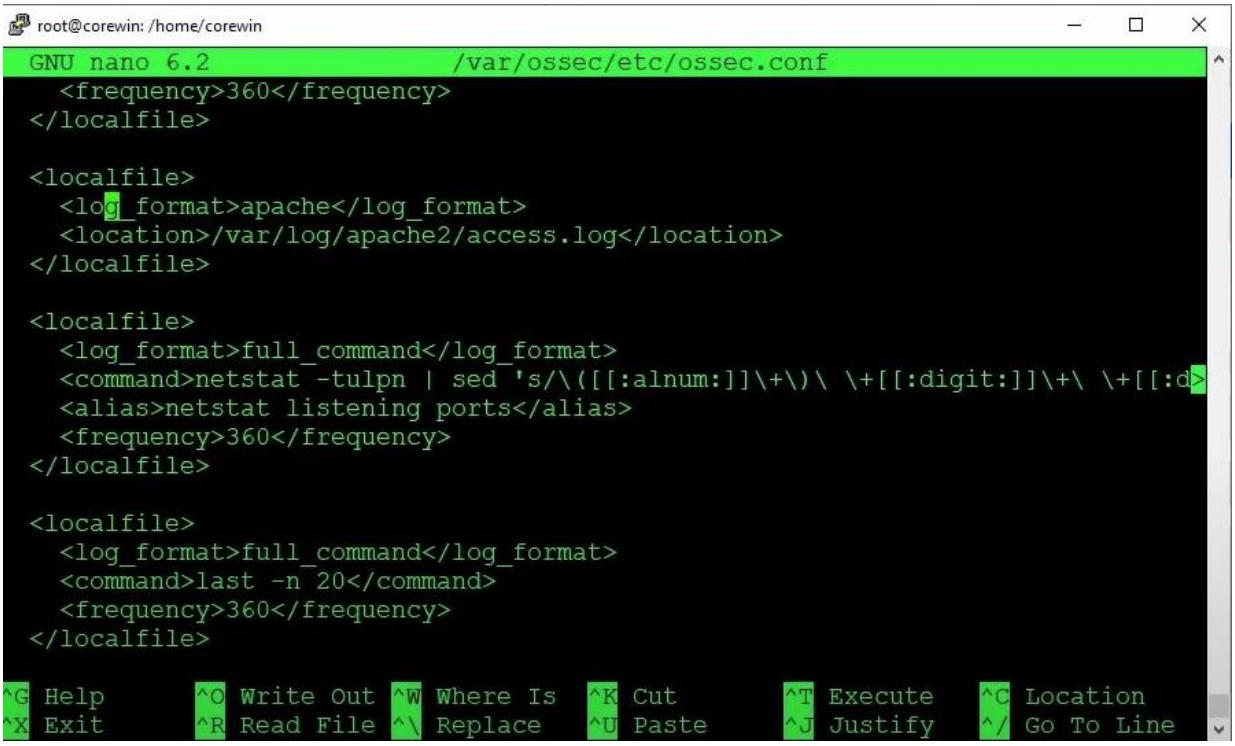


Рисунок 3.16 – Файл з налаштуваннями

Далі потрібно ініціювати атаку. Для цього потрібно відкрити іншу віртуальну машину на базі операційної системи Ubuntu та відправити запит, який буде містити в собі ключові ознаки SQL ін'єкцій (рис.3.17).

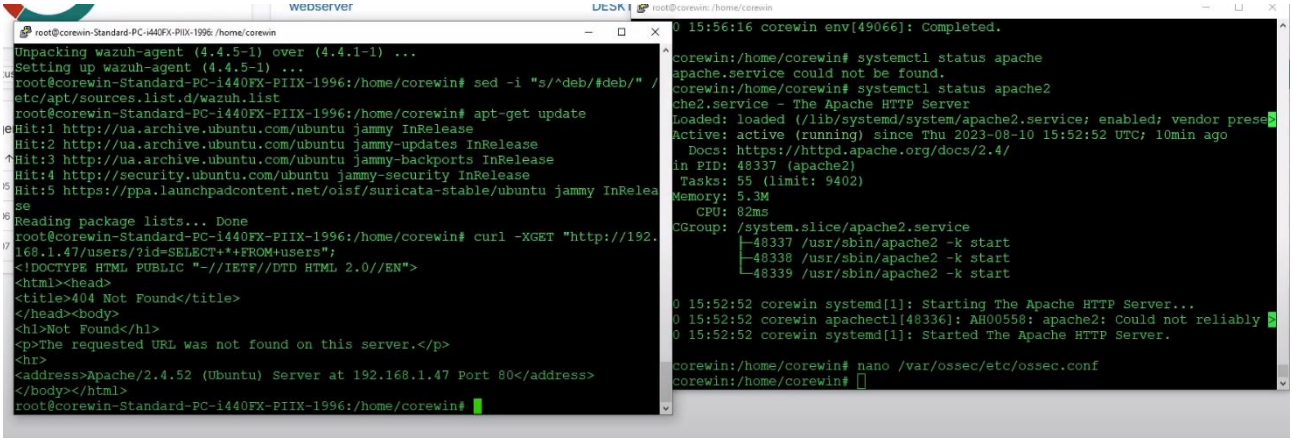


Рисунок 3.17 – Відкриття віртуальної машини

Після відкриття необхідно створити запит, який буде містити в собі ключові ознаки SQL-ін'єкцій. Далі, відповідно, необхідно виконати запит через інструмент *curl*, тобто вбудований інструмент запитів. В даному інструменті виконуємо запит на IP-адресу машини, де стоїть веб-інтерфейс.

Наступним кроком необхідно виконати команди *Select* та *From*, що є одними з ключових ознак виконання SQL-ін'єкцій (рис.3.18).

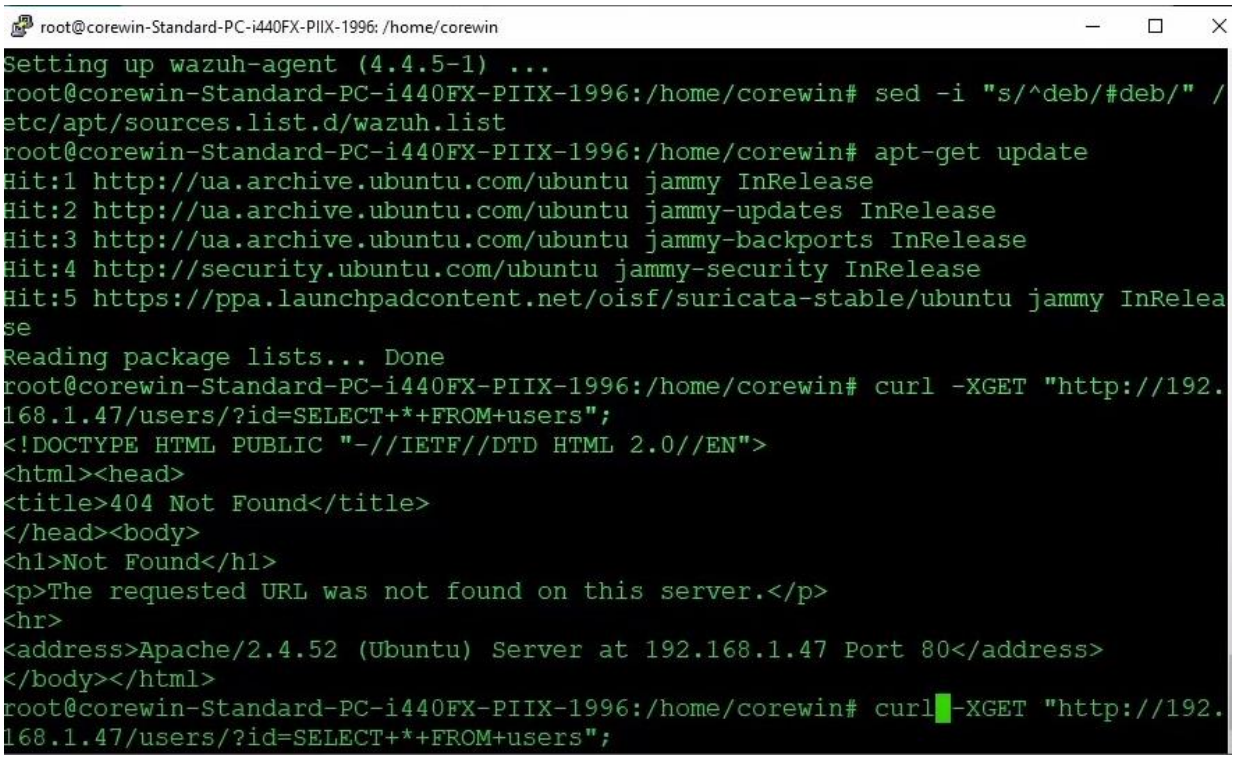


Рисунок 3.18 – Конфігурація

Після воду команди отримуємо відповідь про те, що сервера не існує, але це й не дивно, адже що запит йшов на звичайний стартовий сайт з серверу Apache, яка йде за замовчуванням (рис. 3.19 та 3.20).

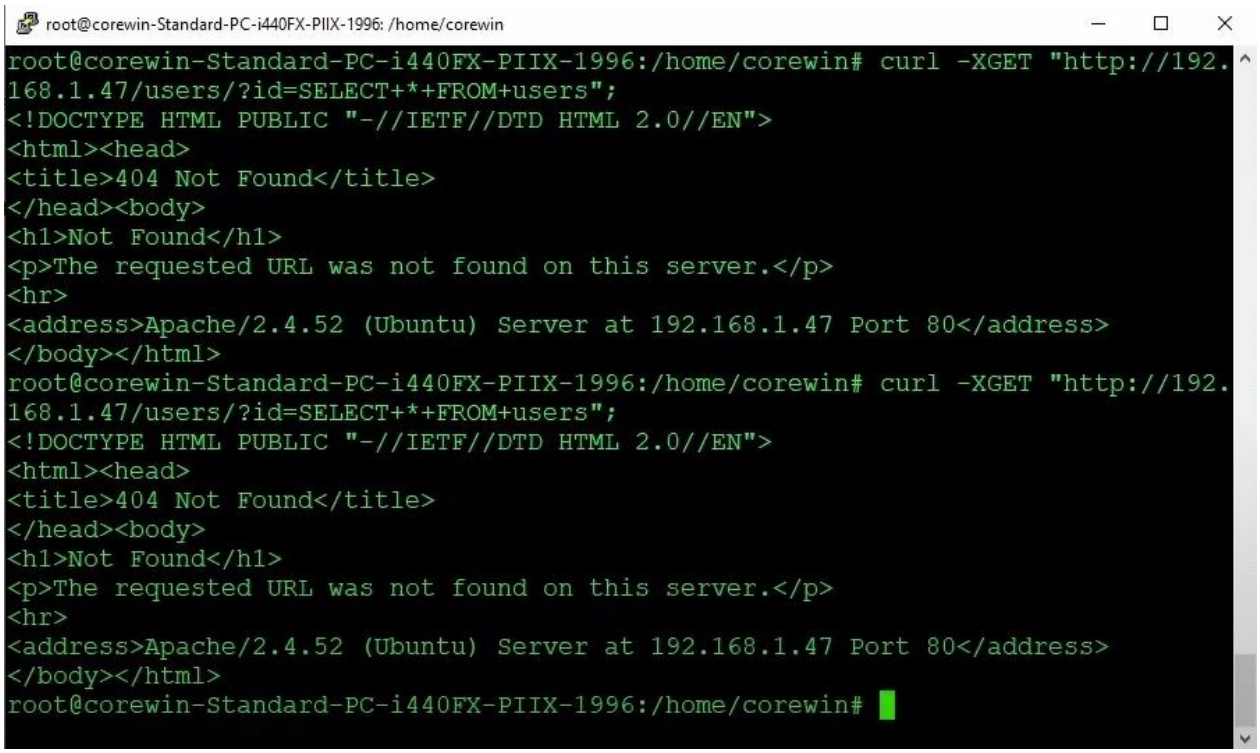


Рисунок 3.19 – Відповідь що сервер не знайдено

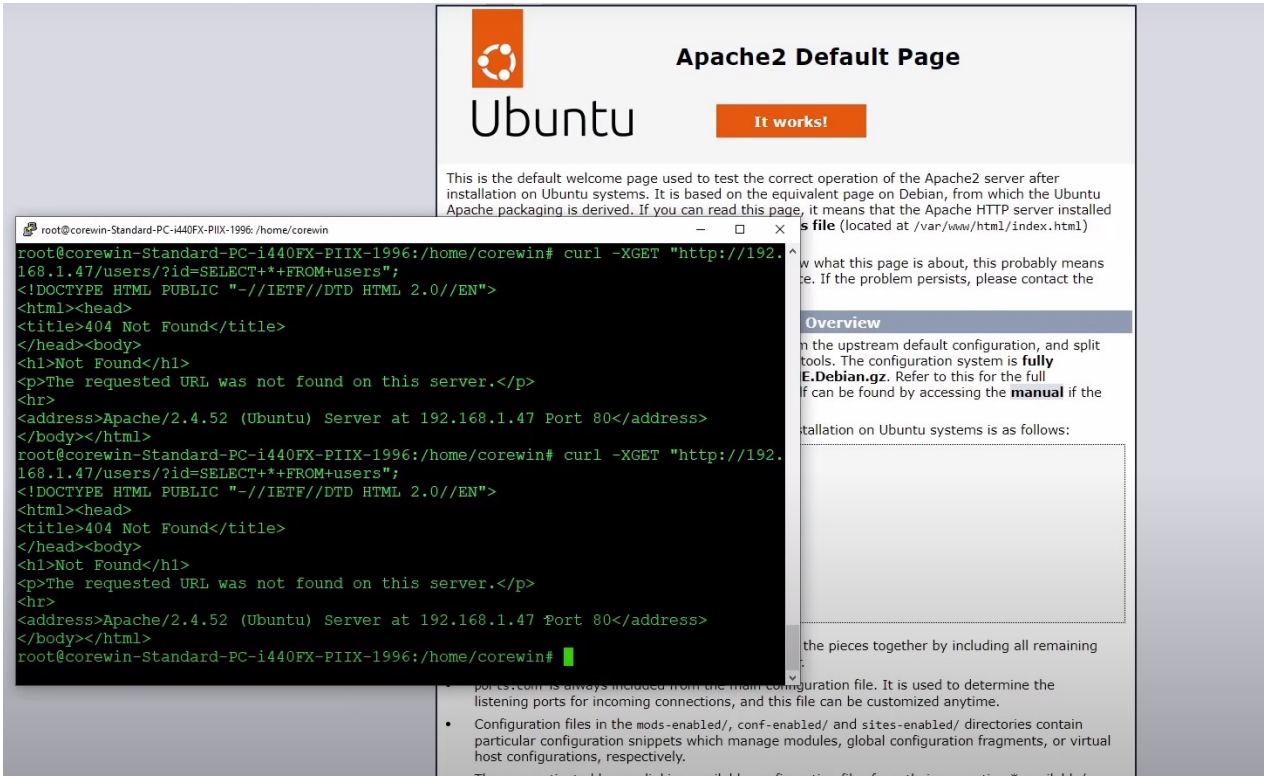


Рисунок 3.20 – Стартова сторінка серверу Apache

Далі потрібно перевірити події. На сервері вони будуть відображені як на діаграмах (рис.3.21), так і у списку з останніми подіями (рис. 3.22).

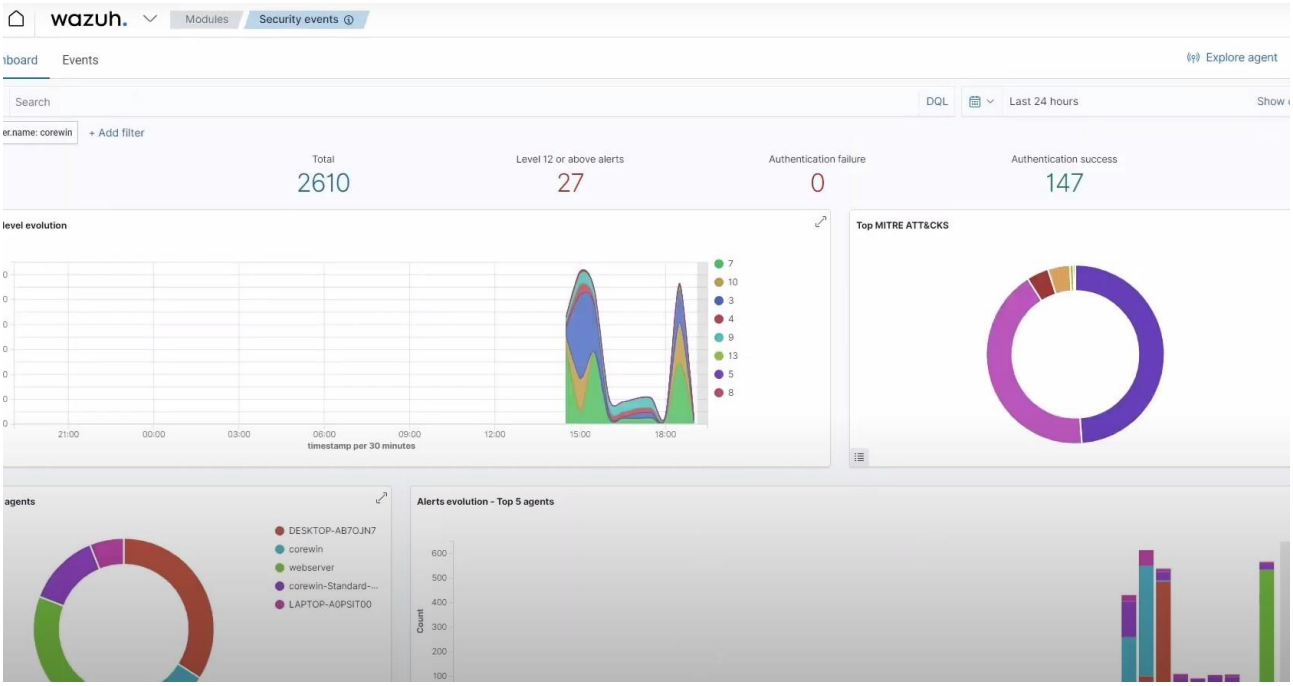


Рисунок 3.21 – Діаграми подій

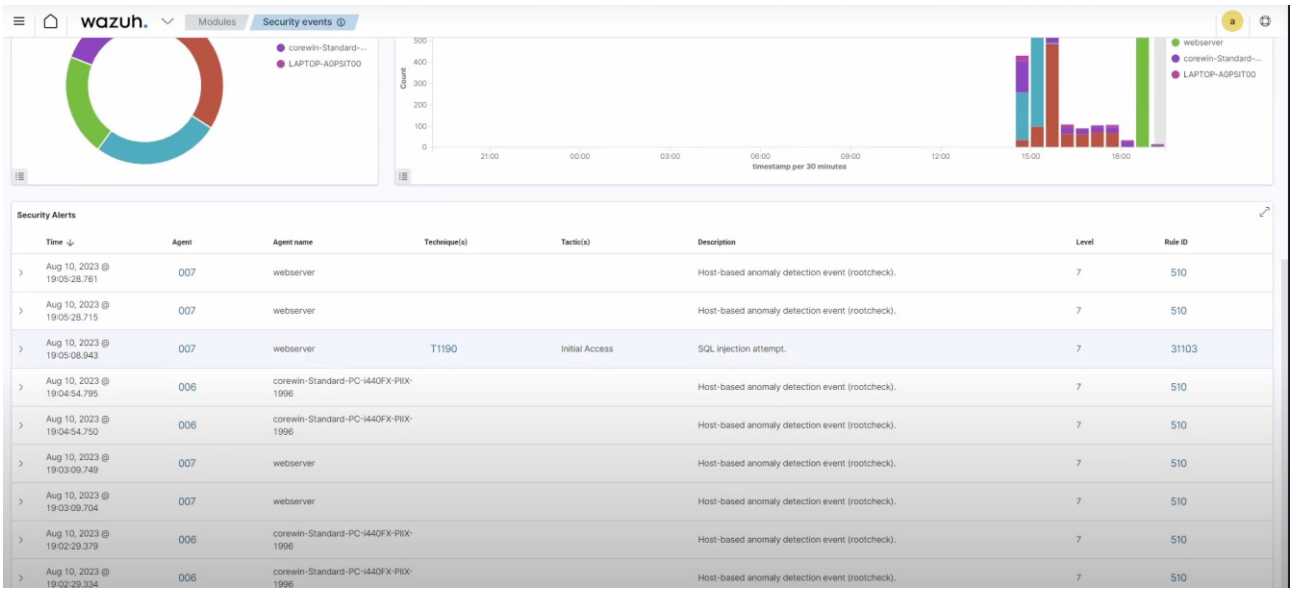


Рисунок 3.22 – Список подій

Як бачимо на попередньому скріншоті, у списку подій була зафіксована ін’єкція. Відповідно до події ми бачимо, що в «Ім’я агента» саме той агент, який стоїть на веб-сервері. Також є можливість розгорнути деталі цієї ін'єкції та зрозуміти звідки була спроба та за допомогою якої саме команди (рис. 3.23).

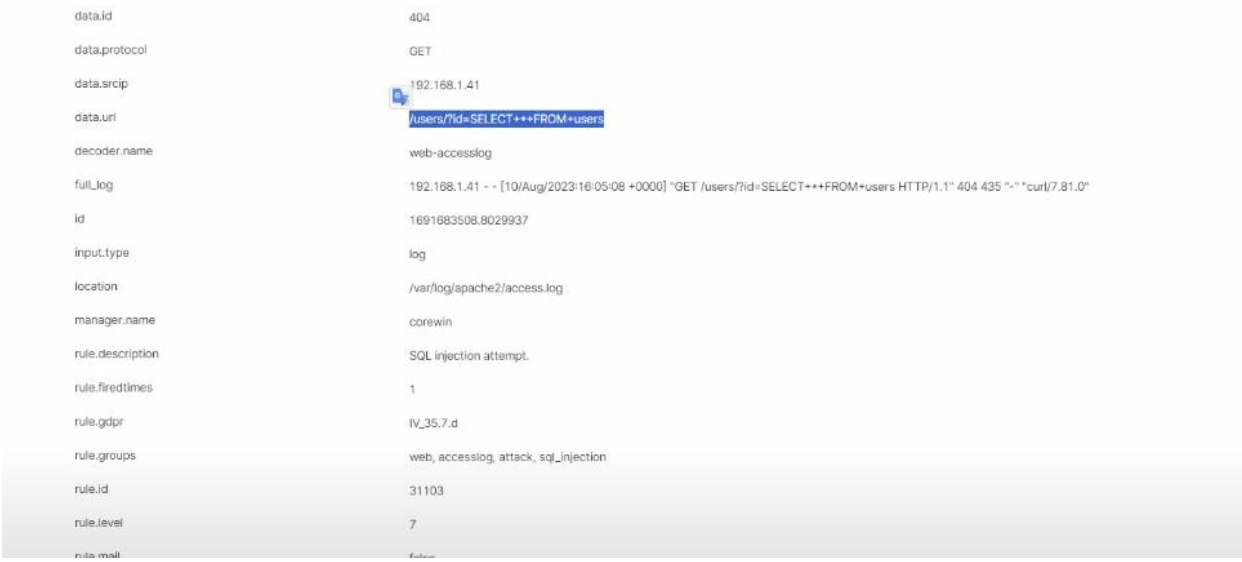


Рисунок 3.23 – Деталі ін’єкції

Важливим моментом є те, що Wazuh є інструменом, який в режимі реального часу зможе відновлювати такі події та оперативно інформувати спеціалістів по безпеці або надавати команду на віддалене виконання, таку як XDR-команду.

3.4 Мережеві вторгнення в Wazuh

Перед початком роботи на систему потрібно інсталювати додатковий компонент, а саме програму «Suricata», котра буде виявляти мережеві вторгнення. Це можна зробити за допомогою пакетного менеджера.

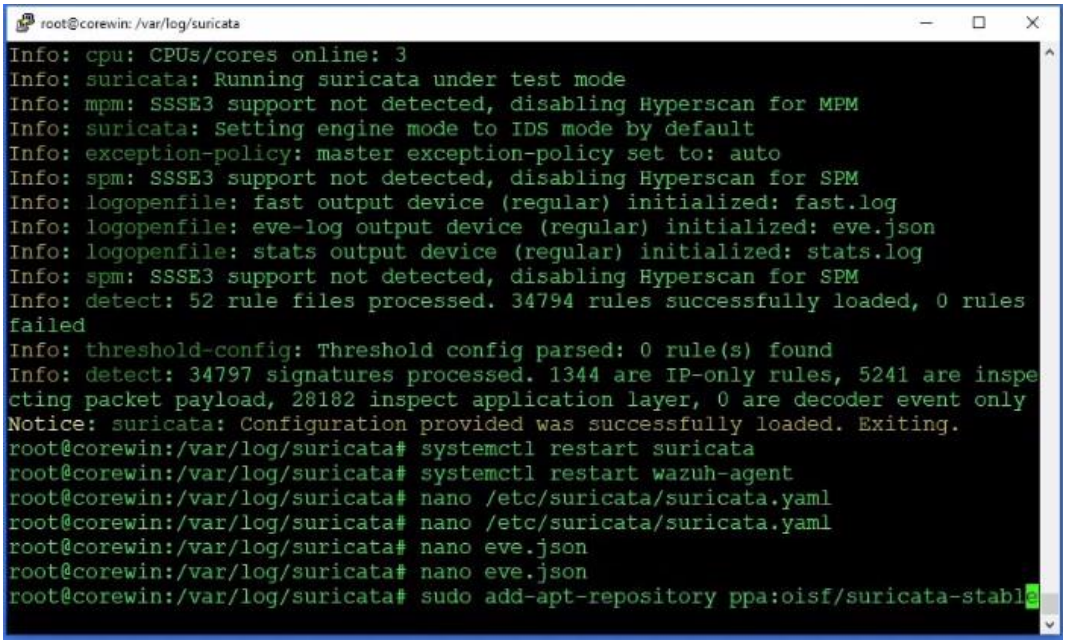


Рисунок 3.24 – Початок завантаження

Процес інсталяції полягає в трьох базових кроках:

- додавання репозиторію;
- оновлення;
- завантаження Suricata (рис.3.25).

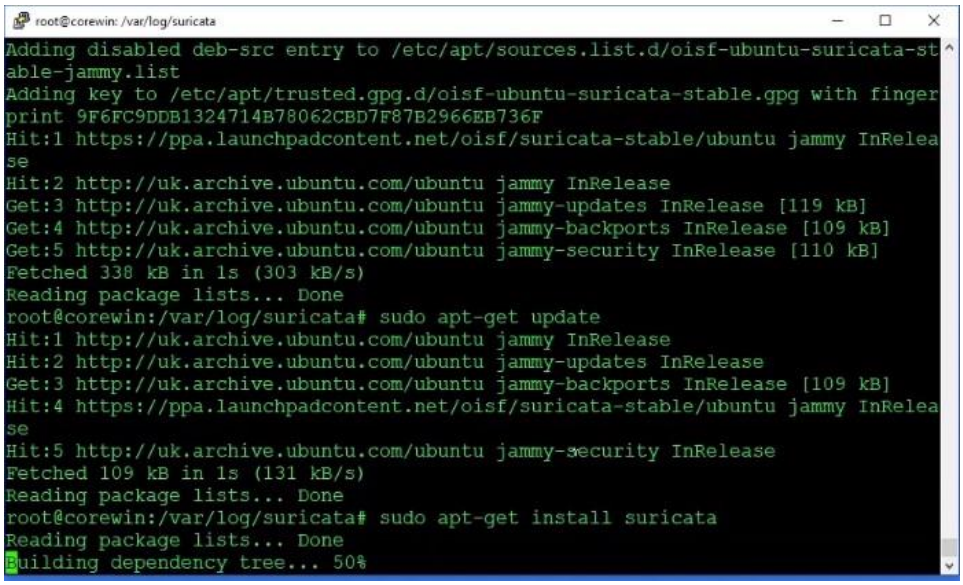


Рисунок 3.25 – Завантаження Suricata

Також необхідно змінити деякі налаштування в конфігурації Suricata. Для цього треба зайти в файл конфігурації.

В налаштуваннях ми визначили домашню мережу та зовнішню мережу, щоб розмежовувати звідки йде трафік – з локальної домашньої мережі чи зовнішнього периметру (рис. 3.26).

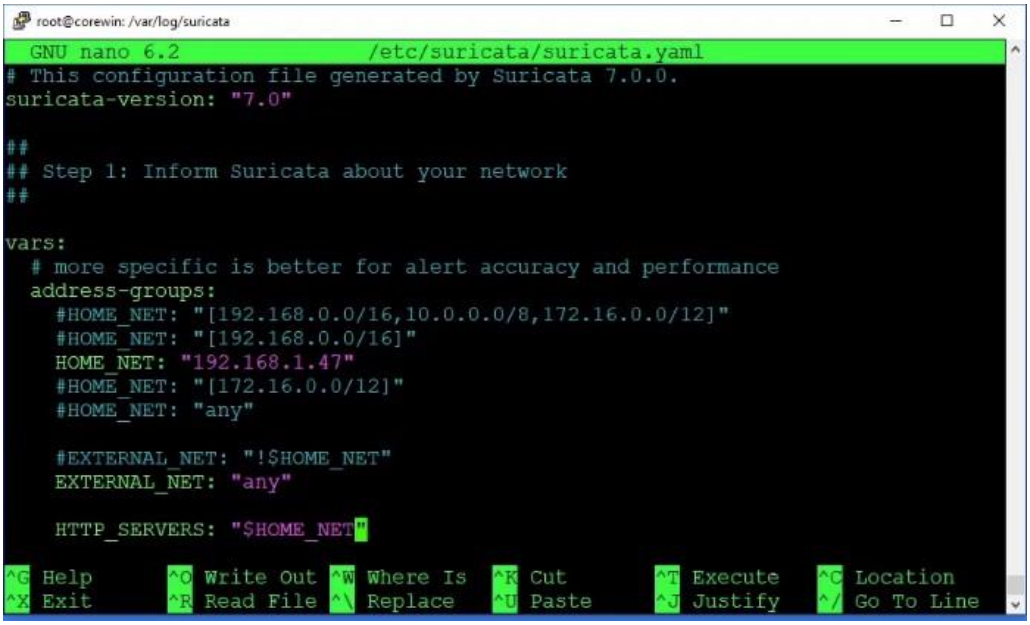


Рисунок 3.26 – Мережі

Додатково була створена додаткова група IDS, до якої було додано агент, на якому виконуємо тестування, та зроблено просту конфігурацію. Інтеграція, в даному випадку, тобто підключення відбувається лише читанням log-файлу та реакцією системи IDS (рис.3.27 та 3.28).

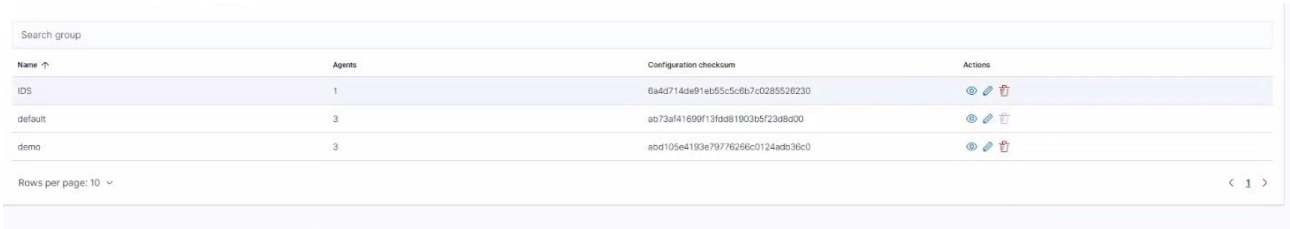


Рисунок 3.27 – Додаткова група IDS

Рисунок 3.28 – Конфігурація

Тепер виконаємо тестову атаку. Для цього буде використана інша віртуальна машина на базі операційної системи Ubuntu.

Атакою може вважатися навіть нетиповий мережевий трафік. В нашому випадку ми будемо пінгувати IP-адресу тривалий час (рис.3.29).

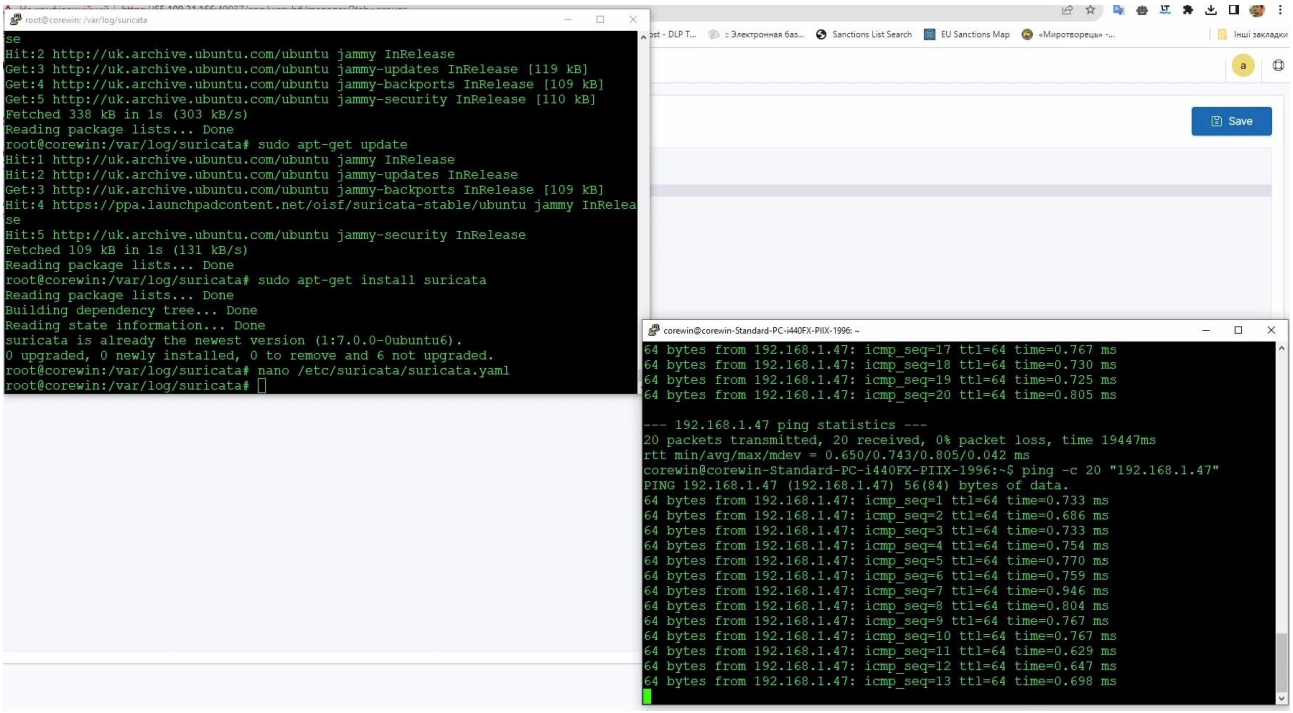


Рисунок 3.29 – Виконання тестової атаки

Після виконання даної атаки Suricata почала аналізувати всі нетипові дії та виводити їх в таблицю. На рис. 3.30 можемо побачити, що в таблицю було виведено нетипові дії, а саме запити по протоколу ICMP та пінгування.

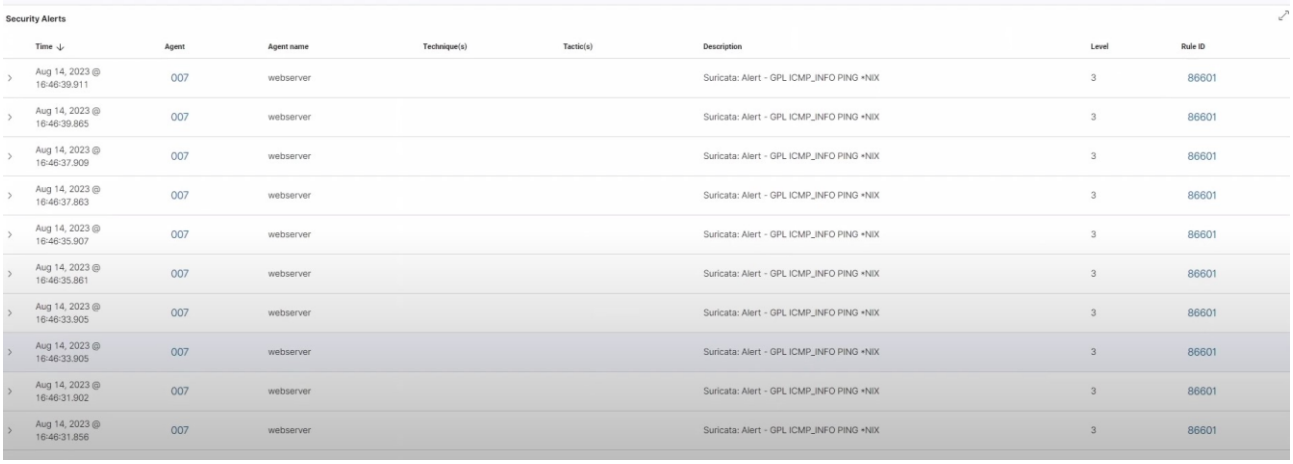


Рисунок 3.30 – Список подій

На рисунку 3.31 можемо бачити деталі даної атаки в таблиці.

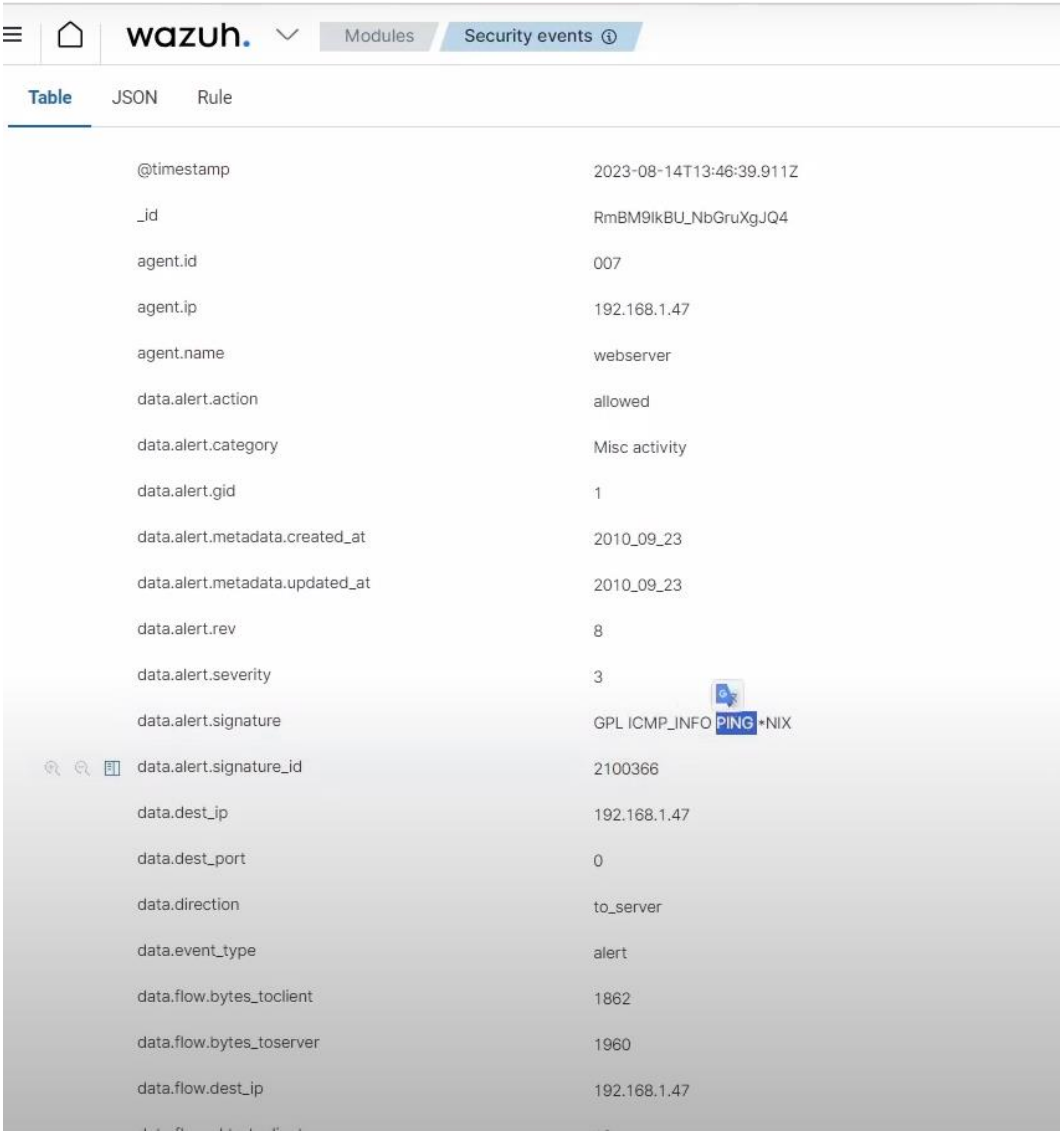


Рисунок 3.31 – Деталі атаки

Suricata ефективно виявляє різноманітні типи атак, включаючи вразливості в мережевих протоколах, атаки на відмову в обслуговуванні (DoS), і спроби використання вразливостей програмного забезпечення. Детальний аналіз журналів Suricata дозволяє визначити характер атак та прийняти заходи для запобігання подібним інцидентам у майбутньому.

Рекомендації щодо підвищення безпеки мережі в даному кейсі включають в себе регулярне оновлення правил виявлення Suricata, моніторинг мережевого трафіку на предмет аномалій, а також впровадження стратегій сегментації мережі та усіх необхідних патчів для програмного забезпечення. Запровадження цих заходів допоможе зменшити ризик мережевих вторгнень та забезпечить стійкість інфраструктури проти потенційних загроз.

Результати даної магістерської роботи було впроваджено в відділі протидії кіберзлочинам в Сумській області (Додаток А).

ВИСНОВКИ

В даній магістерській роботі було проведено глибоке дослідження актуальності та необхідності застосування інформаційних технологій та інструментів для активних дій у кібербезпеці. Аналіз сучасного стану кіберзагроз підкреслив важливість розробки та впровадження ефективних стратегій активного захисту для протидії кібератакам, що постійно еволюціонують.

Дослідження різноманітних інструментів і методів активного захисту, включаючи системи виявлення та запобігання вторгненням (IDS/IPS), аналітику великих даних, та автоматизовані системи реагування на інциденти, продемонструвало їх ефективність у забезпеченні більш високого рівня безпеки.

Розроблена методологія дослідження та аналізу дала можливість глибше зрозуміти потенціал та обмеження сучасних інструментів кібербезпеки. Отримані результати та висновки можуть бути використані для покращення існуючих систем безпеки та розробки нових рішень, що допоможуть протистояти кіберзагрозам на різних рівнях.

Робота також вказує на потребу постійного оновлення знань та навичок у галузі кібербезпеки, оскільки кіберзагрози мають властивість швидко змінюватись та адаптуватись. Рекомендації, представлені у дослідженні, надають основу для розвитку та вдосконалення стратегій кібербезпеки на рівні організацій та індивідуальних користувачів.

У підсумку, дане дослідження вносить значний вклад у розуміння актуальності та важливості активних дій у кібербезпеці, забезпечуючи важливі рекомендації для їх ефективного впровадження та застосування у відповідь на зростаючі кіберзагрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Когут Ю. Кібербезпека та ризики цифрової трансформації компанії : навч. посіб. Консалтинг. компанія Сідкон, 2021. 372 с.
2. Віннікова І. І. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними / І. І. Віннікова, С. В. Марчук // Східна Європа: економіка, бізнес та управління. – 2018. – № 5. – С. 110-114.
3. Blokdyk G. Intrusion Detection Systems A Complete Guide. 2021st ed. 5STARCooks. 225 p.
4. Pathan A.-S. K. The State of the Art in Intrusion Prevention and Detection. Auerbach Publications, 2016. 514 p.
5. Adeyemo A. Design of an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) for the EIU Cybersecurity Laboratory. 3rd ed. Eastern Illinois University, 2016. 178 p.
6. Blokdyk G. Intrusion Prevention System A Complete Guide. 5STARCooks, 2021. 314 p.
7. SNORT–Network Intrusion Detection and Prevention System| Fortinet. Fortinet. URL: https://www.fortinet.com/lat/resources/cyberglossary/snort (date of access: 24.11.2023).
8. How To Configure Suricata as an Intrusion Prevention System (IPS) on Debian 11. DigitalOcean | Cloud Hosting for Builders. URL: https://www.digitalocean.com/community/tutorials/how-to-configure-suricata-as-an-intrusion-prevention-system-ips-on-debian-11 (date of access: 25.11.2023).
9. Cybersecurity Integrations & Tools. cyberCTRL. URL: https://cyberctrl.net/product-integrations/ (date of access: 25.11.2023).

10. 2023 Guide: The 25 Best Intrusion Detection and Prevention Systems. The CTO Club. URL: https://thectoclub.com/tools/best-intrusion-detection-and-prevention-systems/ (date of access: 25.11.2023).

11. Ziegler M. Snort: Executing a Snort rule on a PCAP file: A Step-by-Step Guide. CopyProgramming. URL: https://copyprogramming.com/howto/how-to-run-a-snort-rule-over-pcap-file (date of access: 26.11.2023).

12. Abdulloh, Y., Triyono, J., & Lestari, U. (2020). Pengaruh Penempatan Snort Terhadap Keamanan Jaringan (Studi Kasus Laboratorium Vi Jaringan Kampus 3 Ist Akprind Yogyakarta). Jurnal JARKOM, 8(1).

13. Adam Dwi Ralianto, & Cahyono, S. (2021). Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Intrusi Lalu Lintas di Jaringan. Info Kripto, 15(2). https://doi.org/10.56706/ik.v15i2.10

14. Huels, F. D., & Stoeger, A. S. (2022). Sentinel behavior in captive meerkats (Suricata suricatta). Zoo Biology, 41(1). https://doi.org/10.1002/zoo.21644

15. Lukman, L., & Suci, M. (2020). Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache. Respati, 15(2). https://doi.org/10.35842/jtir.v15i2.343

16. Perdigón, R. (2022). Suricata como detector de intrusos para la seguridad en redes de datos empresariales. Ciencia UNEMI, 15(39). https://doi.org/10.29076/issn.2528-7737vol15iss39.2022pp44-53p

17. Sharma, N. V, Kavita, Aggarwal, G., & Sharma, S. (2021). Performance Study of Snort and Suricata for Intrusion Detection System. IOP Conference Series: Materials Science and Engineering, 1099(1). https://doi.org/10.1088/1757-899x/1099/1/012009

18. Stephani, E., Fitri Nova, & Ervan Asri. (2020). Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server. JITSI : Jurnal Ilmiah Teknologi Sistem Informasi, 1(2). https://doi.org/10.30630/jitsi.1.2.10

19. Syamsuddin, I., & Barukab, O. M. (2022). SUKRY: Suricata IDS with Enhanced kNN Algorithm on Raspberry Pi for Classifying IoT Botnet Attacks. Electronics (Switzerland), 11(5). https://doi.org/10.3390/electronics11050737

20. Syani, M. (2020). IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA PADA LINUX DEBIAN 9 BERBASIS CLOUD VIRTUAL PRIVATE SERVERS (VPS). Jurnal Inkofar, 1(1). https://doi.org/10.46846/jurnalinkofar.v1i1.155

21. Tanang Anugrah, F., Ikhwan, S., & Gusti A.G, J. (2022). Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection. Techné : Jurnal Ilmiah Elektroteknika, 21(2). https://doi.org/10.31358/techne.v21i2.320

22. Zain, A. R., Oktivasari, P., Fauzi Soelaiman, N., & Watsiqul Umam, F. (2023). IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) SURICATA DAN MANAGEMENT LOG ELK STACK UNTUK PENDETEKSIAN KEGIATAN MINING. Jurnal Poli-Teknologi, 22(1). https://doi.org/10.32722/pt.v22i1.4974

ДОДАТОК А

ДОВІДКА

Про впровадження результатів магістерської роботи

Дана студентці групи Ін.м-22 факультету електроніки та інформаційних технологій Сумського державного університету Ященко Анні Миколаївні в тому, що матеріали її магістерської роботи на тему «Інформаційні технології та інструменти активних дій в кібербезпеці», виконаної на матеріалах відділу протидії кіберзлочинам в Сумській області ДКП НПУ, розглянуті.

Окремі розробки авторки, її висновки і пропозиції становлять певний інтерес і прийняті для практичного використання в діяльності відділу протидії кіберзлочинам в Сумській області.

Зокрема:

- огляд та оцінка ефективності інструментів активних дій в кібербезпеці;
- розробка методологічного підходу для реагування мережеві вторгнення та інші види кіберзагроз;
- рекомендації щодо захисту від кіберзагроз та їх попередження.

Т.в.о. начальника
ВПК в Сумській області
ДКП НПУ

Василь ІСАКОВ