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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: Автоматизація аналізу log-файлів для виявлення аномальної поведінки користувача

Виконав(ла): студент(ка) VI курсу, групи СБм-61
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)

(підпис) Іванюк Д.Ю.
(прізвище та ініціали)

Керівник (підпис) Загородна Н.В.
(прізвище та ініціали)

Нормоконтроль (підпис) Кареліна О.В.
(прізвище та ініціали)

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

Рецензент (підпис) Литвиненко О.В.
(прізвище та ініціали)

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

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

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Іванишину Денису Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Лінгвістичний аналіз вебсайтів для виявлення аномальної поведінки користувача

Керівник роботи Загородна Наталія Володимирівна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___» _____ 20___ року № _____

2. Термін подання студентом завершеної роботи 14.12.2021р

3. Вихідні дані до роботи 14.12.2021р. Вебсайти

4. Зміст роботи (перелік питань, які потрібно розробити)
Розробка алгоритмів аналізу вебсайтів; методика системи автоматизації аналізу вебсайтів; тестування системи

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

Розділ	Прізвище, ініціали та посада консу	Підпис	Дата
Охорона праці безпека в надзвичайних ситуаціях	Осухівська І.Ю. Кетчик В.М. ст. викладач		

7. Дата видачі завдання 29.09.2021

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Опрацювання завдання	04.10.2021	Викон
2.	Аналіз літературних джерел	05.10.2021	Викон
3.	Написання першого розділу	10.10.2021	Викон
4.	Розробка ПЗ (аналіз від-фотипів)	10.11.2021	Викон
5.	Написання другого розділу	16.11.2021	Викон
6.	Написання третього розділу	24.11.2021	Викон
7.	Опрацювання питань розділу захисту	01.12.2021	Викон
8.	Оформлення роботи	04.12.2021	Викон
9.	Перевірка на плагіат	14.12.2021	Виконо
10.	Попередній захист	17.12.2021	Викон
11	Захист		

Студент

АНОТАЦІЯ

Автоматизація аналізу log-файлів для виявлення аномальної поведінки користувача// Івашин Денис Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБм–61 // Тернопіль, 2021 // С.–45, рис.–17, ліст. – 2.

Ключові слова: АВТОМАТИЗАЦІЯ, АНАЛІЗ, АНОМАЛЬНА ПОВЕДІНКА

Кваліфікаційна робота присвячена дослідженню автоматичних систем аналізу log-файлів, для виявлення аномальної поведінки користувача. В роботі проаналізовано існуючі види та способи автоматизації аналізу log-файлів, досліджено та описано їх переваги та недоліки. Також в роботі описано принцип автоматизації та аналізу log-файлів.

Було та розроблено автоматизовану систему аналізу для виявлення аномальної поведінки користувача, яка здатна самостійно збирати, аналізувати та фільтрувати дані. На основі цих даних, система здатна надавати результати у вигляді сповіщень про порушення безпеки на відповідній панелі адміністратора мережі.

ANNOTATION

Automation of log-files analysis for abnormal user behavior detection// Ivashyn Denys Yuriyovych// Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security // Ternopil, 2021 // P.–45, pic.–17., list. – 2.

Keywords: AUTOMATION, ANALYSIS, ABNOMAL BEHAVIOR

Qualification work is devoted to the study of automatic log-file analysis systems to detect abnormal user behavior. The paper analyzes the existing types and methods of automation of log-file analysis, researches and describes their advantages and disadvantages. The paper also describes the principle of automation and analysis of log files.

An automated analysis system has been developed to detect abnormal user behavior, which is able to independently collect, analyze and filter data. Based on this data, the system is able to provide results in the form of security breaches on the appropriate panel of the network administrator.

ЗМІСТ

ВСТУП

В сучасному світі комп’ютерні системи використовуються для ефективного виконання різного роду задач у різних галузях людського життя. Широко використовуються об’єднання комп'ютерів у мережі, що утворюють розподілену систему для створення паралельних обчислювальних систем. Це може бути дуже масштабною системою, яка в свою чергу потребує ефективного способу захисту, не є винятком також дуже малі системи. попри ряд переваг, до яких належать масштабованість, паралелізація, відмовостійкість, використання таких складних комплексів має ряд недоліків, в тому числі пов’язаних з безпекою. Зокрема, створення розподілених систем підвищує складність для відслідковування всіх подій, які становлять небезпеку компрометації даних, тому система моніторингу подій є одним із загальноприйнятих підходів захисту інформації в інформаційно-комунікаційних системах.

IDS (Intrusion Detection System) - це програмні або апаратні системи, які автоматизують процес перегляду подій, що виникають у комп'ютерній системі чи мережі та аналізують їх з точки зору безпеки. Так як кількість мережевих атак зростає, IDS стають необхідним доповненням інфраструктури безпеки.

На даний момент існує багато систем моніторингу подій, але майже всі вони націлені на великі комп’ютерні системи та мережі і є дуже ресурсо-затратними для звичайних ПК. Звісно ж існують системи із мінімальними вимогами до ресурсів ПК, але зазвичай вони мають недостатньо функціоналу для виявлення кіберзагроз.

Дана робота зосереджена на створенні автоматичної системи моніторингу подій, для запобігання порушення цілісності, доступності та конфіденційності інформації та є цілком безкоштовною із усім необхідним функціоналом. Тому, що в ІКС процесу захисту інформації потрібно приділяти увагу, ще на початку розробки такої системи. Адже дуже важливим є створення системи яка матиме належний функціонал, який не вимагатиме великої кількості системних ресурсів та буде відносно дешевим в обслуговуванні.

Об’єктом дослідження в даній роботі є log-файли.

Предметом дослідження є автоматизація аналізу log-файлів.

Метою роботи є розробка автоматизованої системи аналізу log-файлів, яка самостійно здатна збирати, аналізувати дані, та на основі аналізу цих даних створювати сповіщення про спроби кіберзагроз чи спроб несанкціонованого доступу до системи.

Для виконання поставленої мети було поставлено низку завдань:

- дослідження методів автоматизованого аналізу log-файлів;
- огляд існуючих способів аналізу log-файлів, їх переваги та недоліки;
- аналіз механізмів роботи автоматизації;
- аналіз способів розробки системи автоматизації аналізу log-файлів;
- розробка алгоритмів аналізу log-файлів, з врахуванням сформованих вимог до нової системи
- побудова системи автоматизації аналізу log-файлів.
- тестування роботи системи автоматизації аналізу log-файлів.

Велика кількість існуючих автоматизованих систем – дорогі в обслуговуванні та є досить ресурсозатратними, і потрібно досягти максимальної ефективності при найменшій ціні.

1 АНАЛІЗ АВТОМАТИЗОВАНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

1.1 Передумови створення автоматизованих систем виявлення вторгнень

З появою сучасних технологій інтернет-комунікація стала дуже ефективною та надійною, але в той же час кібератаки стають все більш розвиненими та витонченими. На цьому тлі, мережева безпека організації стає основним предметом захисту. У таких інфраструктурах, як електроенергетика та енергетика, які мають як фізичний, так і кібернетичний рівень важливу роль відіграє автоматизація всіх можливих процесів задля спрощення та полегшення важкої та рутинної роботи. Сучасне суспільство дуже залежить від систем комунікації та звісно від самих засобів комунікації, і будь-який значний вплив на критичну інфраструктуру може порушити її стабільність. Скоординована кібератака, як-от 2015 Ukraine blackout, може призвести до відключення електроенергії, що вплине на близько 225 000 клієнтів. Шкідливі програми, такі як Stuxnet, заражали промислові системи контролю, вироблені Siemens, створюючи порушення в процесах управління центрифуг іранського ядерного реактора. Доступність і цілісність даних стає однією з головних проблем у промислових комунікаціях. Це створює потребу в досягненні високобезпечного та надійного захисту інформації. Сучасні організації використовують Інтернет по-різному, їх безпека першого порядку — це брандмауер, IDS, IPS, керування інцидентами та подіями безпеки (SIEM) та аналітика даних. Використання розширеного брандмауера, який має фільтрацію прикладного рівня, може уникнути більшості кібератак. З іншого боку, кібератаки розвиваються все більш приховано. Системи виявлення та запобігання вторгненням, наприклад, на основі правил, аналізу та поведінки, допомагають виявляти зловмисників у реальному часі. Також існує велика потреба в моніторингу мережевої активності для аналізу мережевої поведінки системи, яка має аномальну поведінку. Крім того, пропускна здатність і статистика використання мережі постійно

відстежуються, щоб виявити будь-яку ненормальну поведінку системи. Коли організація має кілька напрямків, перед її операціями стоїть складне завдання – керувати мережею клієнтів. Головною проблемою залишається захист їхніх офіційних даних у кількох областях з єдиної точки зору, що призводить до розподіленої системи виявлення та запобігання вторгненням. Стандартизація безпеки має різну перспективу для середовищ IT та ОС, оскільки ризики різні в різних областях. Весь системний процес залежить як від кіберзагроз, так і від фізичних процесів, будь-які розбіжності в часі між сервером і клієнтом можуть призвести до катастрофічних наслідків. Оскільки ОС використовують датчики для регулювання критичних процесів і пов’язані із застарілими системами, пріоритет доступності є вищим, ніж цілісність і конфіденційність [1].

Мережеві дані, якими обмінюються через комунікацію SCADA (Supervisory Control And Data Acquisition), мають велике значення для доступності, цілісності та конфіденційності. У цьому порядку, доступність є надзвичайно важливою, оскільки всі процеси, якими керують і які контролюються, відбуваються в режимі реального часу. У традиційній безпеці конфіденційності та цілісності повідомлення надається більше значення. Однак у критичних комунікаціях, доступності пакетів даних надається першочергове значення. Також потрібно не забувати про цілісність, де дані, якими обмінюються сервер і клієнт, повинні підтримуватися високою інтеграцією. Будь-яке порушення у відношенні до цілісності отриманих даних може призвести до катастрофічних наслідків. Конфіденційність має найнижчий пріоритет порівняно з двома іншими. Передача даних у більшості середовищ SCADA не зашифрована, оскільки шифрування створює додатковий час, що перешкоджає доступності критичного зв’язку [2].

1.2 Принципи роботи IDS

Багато існуючих мереж уразливі до кібератак через відсутність належної безпеки. Застосовувати заходи безпеки IT до операційного середовища не є практичним підходом, оскільки доступність більше стосується промислових

систем управління. Мережа SCADA має головний сервер для підключення до клієнта на виїзних станціях для виконання операцій у режимі реального часу, і підключений для забезпечення механічної стабільності. З'являється різноманітність загроз, що здійснюються різними суб'єктами або діяльність за підтримки незаконних груп на мережу чи систему, яким керує SCADA. На даному етапі дуже важливо забезпечити надійні технології для запобігання зловмисної діяльності та безпечного зв’язку SCADA. Приховані кібератаки, такі як спуфінг IP, можуть маніпулювати всім мережевим заголовком пакета і можуть обійти існуючі заходи безпеки. Системі брандмауера та виявлення вторгнень не вистачає можливостей виявлення атак-спуфінгу на основі IP. Використання застарілої інфраструктури відкриває достатній простір для використання зловмисниками різного роду шкідливого програмного забезпечення за допомогою сучасних інструментів і технологій [3].

Традиційну архітектуру, яка використовується для створення критичних систем, важко сучасних до сучасних технологій. Оскільки, якщо інфраструктура збирається трансформуватися, необхідно подолати багато обмежень, це вимагає величезних зусиль і змін технологій аналізу, що використовується в нинішніх технологіях [4].

Для боротьби з небажаною кіберактивністю застосовано багато технологій. IDS в мережі служить пристроєм, який безперервно відстежує події мережевого трафіку і не тільки. IDS також аналізує поведінку системи та захищає системи від несанкціонованого доступу. Основним напрямком цієї роботи є забезпечення автоматизованої системи виявлення та запобігання вторгненням у мережі для фільтрації та реєстрації вхідного та вихідного трафіку. Ця розширена функціональність забезпечує виявлення сигнатур загроз, виявлення вірусних сигнатур, а також захист на рівні мережі та рівня програм. На відміну від традиційних брандмауерів, IDS з IPS має кращу видимість і контроль у режимі реального часу. Існують різні типи IDS, наприклад IDS на основі аномалій і IDS на основі сигнатур. Ця робота зосереджена на IDS на основі аномалій. За допомогою цього методу виявляються неправомірні дії в мережі та на хостах. На

підставі історії нормальної роботи хоста та мережі створюються спеціальні профілі з даними про це. Потім до гри вступають спеціальні детектори, які аналізують події. З допомогою різних алгоритмів вони проводять аналіз цих подій, порівнюючи їх з «нормою» у профілях. Відсутність потреби накопичувати безліч сигнатур атак – безперечний плюс цього способу. Проте чимало хибних сигналів про атаки при нетипових, але цілком законних подіях у мережі – це безсумнівний його мінус [5].

1.3 Структура автоматизованих систем виявлення вторгнень

Структура IDS може бути двох типів централізована або розподілена. Централізована IDS діє як окрема система без взаємодії зі своїми клієнтами. У розподіленій установці мережа складається з кількох клієнтів IDS, які підключаються до головного IDS. Моніторинг розподіленої мережі дає змогу переглядати загальну мережеву активність із головної консолі. Це надає адміністратору мережі гнучкість для покращення моніторингу мережі та керування різними мережами та вжиття профілактичних заходів у режимі реального часу. Завдяки такому налаштуванню адміністратор мережі може значно зменшити ймовірність атаки та збільшити видимість і контроль над кількома областями мережі. Однак брандмауери на шлюзі комунікації SCADA додаються до білого списку відповідно до IP-адрес, програм, веб-сайтів, користувачів, процесів, пристроїв, щоб обмежити небажаний доступ. Крім того, брандмауери додають решту до чорного списку, де будь-яку підозрілу активність, виявлену в будь-якому додатку, користувачах, IP-адресах, веб-сайтах, можна негайно заблокувати. Брандмауер наступного покоління має розширені функції, такі як білий список і чорний список на рівні фізичних MAC-адрес, мережі та рівня програм. У цій топології всі кінцеві точки розглядаються як клієнти, а адміністратор контролює всіх клієнтів. Основною особливістю цієї роботи є надання адміністратору мережі повного контролю подій на єдиній панелі керування. В основному він спрямований на захист кожної кінцевої точки,

застосовуючи політику для блокування небажаних спроб доступу та іншої ризикованої діяльності в цих точках входу. Він може підтримувати більший контроль над точками доступу до мережі та ефективніше блокувати загрози. Він також надає розширені функції, такі як моніторинг та блокування ризикованих або шкідливих дій. Мережевий зв'язок, що включає критичні команди, має певну часову послідовність, яку можна назвати аналізом поведінки системи. Враховуючи всі вищезазначені міркування, створюється алгоритм, який показує генерацію правил IDS. Після генерації правила система виконує початкові операції. Потім проводять різноманітні кібератаки для перевірки працездатності алгоритму генерації правил IDS. Це підтверджується шляхом спостереження за тим, чи може набір правил IDS виявити численні кібератаки в межах заданого діапазону. Після цього розгортання та тестування, порядок набору правил ретельно перевіряється. Два типи порядку правил використовуються для перевірки мінімального часу виявлення, потім порівнюються з графічними термінами. Нарешті, пропонується дійсний порядок послідовності правил з алгоритмом генерації правила в заданій області та оцінка з достатньою кількістю результатів [6].

Роботу промислової системи керування можна підсумувати як передачу даних між датчиками, ПК та іншими пристроями в цій галузі в режимі реального часу. IDS відіграє важливе значення в управлінні обладнанням і системами. На тлі існуючих кіберзагроз атаки, пов’язані з цими інфраструктурами, збільшуються через використання застарілої інфраструктури та вразливості традиційних архітектур і протоколів. Протоколи зв’язку, що використовуються в промисловій системі керування (ICS), такі як DNP3, Modbus, IEC 61850, мають наявні вразливості. Зв’язок, який відбувається між різними вузлами в мережі, вимагає розподіленої системи виявлення вторгнень. Щоб захистити від кібератак, потрібно отримати уявлення про діяльність мережі в режимі реального часу. Вимоги щодо системи виявлення, яка зв’язується з центральним вузлом з усіх мереж, є дуже очікуваною. Використовуючи розроблені правила IDS,

показано, як зменшити ймовірність атаки, використовуючи інформацію інструментів [7].

1.4 Архітектура системи виявлення вторгнень

Використання розподілених систем виявлення вторгнень дає оператору кібермережі можливість контролювати мережу своїх станцій. Це полегшує роботу оператора за рахунок надання єдиної консолі перегляду всієї його мережі, таким чином оператор може потенційно використовувати цю функцію в інтелектуальній мережі. Розподілена архітектура IDS, включає один головний вузол і багато датчиків. Усі прямі вузли підключені до головного вузла. У Клієнта встановлено ПЗ, яке працює в безладному режимі для збору інформації про мережу та її пересилання до адміністратора. У автономній роботі головний вузол має свій сервер бази даних. Тоді як у розподіленому розгортанні є дві архітектури. З розгортанням вузла зберігання чи без нього. Під час розгортання вузла розподіленого сховища головний утримує вузол зберігання для пересилання інформації мережевих даних для майбутніх запитів. Зберігання цих аналітичних даних корисно для аналізу станів системи та поведінки процесу для виявлення будь-якої ненормальної поведінки. Розширене машинне навчання використовує аналітику даних для підготовки належної моделі для IDS. Іншою особливістю використання цієї розподіленої IDS є набори правил, які можна налаштовувати. Правила IDS розроблені на основі шаблону трафіку, мережевих пакетів, потоку пакетів, вмісту пакетів і порогового часу пакету; це одна з найважливіших характеристик, яку можна адаптувати для різних типів середовищ. Ця потенційна функція надає експерту з кібербезпеки величезну гнучкість для аналізу та моніторингу даних мережі з єдиної станції. Крім того, оператор може використовувати гнучкість написання різних типів правил IDS, які відповідають його мережевому середовищу [8].

У налаштуваннях розподілу ми розглядаємо різні типи вузлів відповідно до відповідних функцій. Вузли класифікуються на головний вузол, вузол датчика

(хост на якому встановлене відповідне ПЗ для збору інформації, вузол зберігання [9]. Головний вузол: при автономному розгортанні головний вузол функціонує так само, як і сенсорний вузол. У розподіленому розгортанні ми маємо головний вузол і кілька сенсорних вузлів. Усі сенсорні вузли, такі як вузол прямого доступу та вузол зберігання, підключені до головного вузла. Головний вузол контролює роботу своєї розподіленої мережі. Усі вузли датчика мають з'єднання безпечної оболонки (SSH) з головним вузлом для зв'язку. Будь-яке оновлення правил IDS, оновлення безпеки мережі, оновлення хосту вторгнення, зроблені на вузлі адміністратора, потім легко передається на вузол зберігання. Це забезпечує гнучкість для адміністратора мережі, щоб надсилати оновлення для різних клієнтів з одного вузла. Функція моніторингу та контролю оновлень IDS робить розподілене налаштування більш зручним у використанні [10]. Як тільки будь-яка із сигнатур правил IDS збігається з мережевим пакетом, механізм виявлення негайно надсилає сповіщення адміністратору мережі. Потім сповіщення можна візуалізувати на інформаційній панелі головного вузла. Вузол зберігання: Вузол зберігання — це додатковий вузол, підключений до головного, де всі журнали мережевого трафіку пересилаються від датчика до головного вузла, а потім головний вузол пересилає журнали до вузла зберігання. Після того як сенсорний вузол фіксує весь мережевий журнал та інформацію, для зберігання цієї інформації потрібен величезний обсяг пам'яті, що є проблемою для головного вузла, і виконання цього в головному вузлі може скоротити час обчислення попереджень про вторгнення та знизити продуктивність. Тому використовується вузол зберігання [11]. Цей вузол працює як сервер бази даних, коли головний вузол запитує будь-яку інформацію, він бере інформацію з вузла зберігання. Вузол зберігання зберігає всі журнали і використовується як аналіз даних для розширеної статистики та аналізу різної поведінки мережі. Головний вузол використовує вузол зберігання для даних, які можна запросити за допомогою міжкластерного пошуку.

2 ПРОЕКТУВАННЯ СИСТЕМИ IDS ДЛЯ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ДІЙ

Перш ніж приступити до розробки системи IDS, потрібно визначити, за яким принципом буде працювати цей модуль, його логіку, структуру та функціонал. Існує декілька видів та способів реалізації IDS.

2.1 Автоматизований аналіз

Автоматизований аналіз — це аналітична здатність автоматично виявляти відповідні аномалії, закономірності та тенденції та надавати користувачам інформацію в режимі реального часу, він не вимагає ручного аналізу користувача чи втручання IT. Нові технології, такі як штучний інтелект (AI), алгоритми генерації природної мови (NLG) і машинного навчання (ML), використовуються для постійного моніторингу операційної продуктивності, відстеження визначених користувачем показників і пошуку у великих наборах даних критичних факторів, які відповідають бажаним результатам бізнесу. Потім він генерує сповіщення про будь-які помітні зміни через фіксовані проміжки часу або тригери та надає проаналізовані результати користувачам [12].

Автоматизована аналітика схиляється до аналізу на основі часових проміжків і зосереджується на змінах у певних категоріях, таких як середнє та загальне значення, напрямок тренду, волатильність, зміни кроків та викиди, такі як стрибки та падіння. Як додаткову функцію, користувач може налаштувати параметри пошуку та сповіщень, щоб вони зосередилися на дуже конкретних показниках, швидше і в більшій кількості, ніж користувачі можуть аналізувати вручну за допомогою звітів самообслуговування та інформаційних панелей [13].

Зрештою, автоматизована аналітика дає змогу аналітикам і користувачам робити швидкі висновки. Він надає ширший і більш динамічний аналітичний досвід і служить доповненням, а не заміною традиційного аналізу аналітики

самообслуговування, пропонуючи ще один потужний шлях для виявлення ідей та дій [14].

Надання користувачам потужної можливості для автоматизованого аналізу та моніторингу на додаток до інструментів, які вони використовують для ручного самообслуговування, є необхідним для виявлення і прийняття рішень [15]. Автоматизована аналітика пропонує переваги як постачальникам програмного забезпечення, так і кінцевим користувачам, і її можна використовувати для різноманітних сценаріїв, таких як виявлення моделей шахрайства, відстеження змін у поведінці клієнтів і надсилання сповіщень про ключові досягнення [16].

Незалежні постачальники програмного забезпечення та корпоративні організації можуть знизити витрати та підвищити рентабельність інвестицій за допомогою автоматизованої аналітики, оскільки їхня аналітична платформа може завчасно виявляти проблеми, тому як користувачі, так і адміністратор можуть запобігти або вирішити їх до того, як вони стануть потенційними проблемами, що призведе до меншого ризику та непотрібних витрат. Можливість швидко реагувати на зміни в даних підвищує гнучкість та дозволяє аналітикам і користувачам зосередитися на інших пріоритетах, заощаджуючи час завдяки автоматичному виявленню та наданню інформації [17].

Для кінцевих користувачів автоматизована аналітика надає більш релевантну та персоналізовану статистику, оскільки її можна попередньо налаштувати для моніторингу, відстеження та надання результатів користувачам на основі того, які показники є найважливішими для них в режимі реального часу та набагато швидше, ніж те, що можна було б зробити вручну та виконується лише за допомогою традиційних інструментів самообслуговування. Інтелектуальний дизайн, запропонований за допомогою алгоритмів машинного навчання, також може створити поведінкову базу для найважливіших метрик, що з часом підвищує точність і створює більш релевантні сповіщення, що заощаджує час і зусилля на їх виявлення.

2.2 Типи реалізації розгортання IDS

Автономне розгортання складається з одного вузла, який поєднує функції головного вузла та вузла зберігання. Цей тип реалізації використовується, якщо зона мережі обмежена. Він використовується локально для керування та моніторингу мережі для тестування. Цей тип розгортання використовується для тестування в лабораторіях та для оцінки. Цей тип розгортання корисний для організацій, які мають обмежені області мережі.

Розподілене розгортання складається з одного головного вузла, одного або кількох прямих вузлів, одного чи більше вузлів зберігання. Ця архітектура широко поширена в виробничій галузі, оскільки вона забезпечує більшу масштабованість, продуктивність, а також обробляє інтенсивний мережевий трафік і керування журналами. Рекомендується використовувати розподілене розгортання для виробничої мережі, а використання вузла зберігання надає більш розширені можливості для вивчення аналізу і пошуку даних [18].

2.3 Методологія виявлення підозрілої діяльності в системі

Основна мета IDS – виявити шкідливу мережеву активність і попередити адміністратора. IDS використовує підписи для узгодження мережевих пакетів для пошуку сповіщення. Коли цей IDS розміщено на шлюзі мережі або в мережі до якої належить пристрій, він може працювати як система запобігання. Система запобігання вторгненню здатна виявляти та захищати від різних типів кібератак, таких як відмова в обслуговуванні. Такий тип реалізації є однією з переваг для адміністратора, оскільки забезпечує функціональність виявлення та запобігання шкідливих дій.

IDS бувають різних типів і виявляють підозрілу діяльність за допомогою різних методів, зокрема таких:

– Система виявлення вторгнення в мережу (NIDS) розгортається в стратегічній точці або точках в мережі, де вона може контролювати вхідний і вихідний трафік з усіх пристроїв мережі.

– Система виявлення вторгнень (HIDS) працює на всіх комп’ютерах або пристроях у мережі з прямим доступом як до Інтернету, так і до внутрішньої мережі підприємства. HIDS має перевагу перед NIDS в тому, що він може виявляти аномальні мережеві пакети, які надходять з середини організації, або шкідливий трафік, який NIDS не зміг виявити. HIDS також може ідентифікувати шкідливий трафік, який походить із самого хоста, наприклад, коли хост був заражений шкідливим програмним забезпеченням і намагається поширитися на інші системи.

– Система виявлення вторгнень на основі сигнатур (SIDS) відстежує всі пакети, що потрапляють в мережу, і порівнює їх з базою даних сигнатур атак або атрибутів відомих шкідливих загроз, подібно до антивірусного програмного забезпечення.

– Система виявлення вторгнень на основі аномалій (СНІД) відстежує мережевий трафік і порівнює його з встановленим базовим рівнем, щоб визначити, що вважається нормальним для мережі щодо пропускної здатності, протоколів, портів та інших пристроїв. Цей тип часто використовує машинне навчання для встановлення базової та супутньої політики безпеки. Потім він попереджає адміністратора мережі про підозрілу діяльність і порушення політики. Виявляючи загрози за допомогою широкої моделі замість конкретних сигнатур і атрибутів, метод виявлення на основі аномалій покращує обмеження методів на основі сигнатур, особливо при виявленні нових загроз.

Історично системи виявлення вторгнень класифікувалися як пасивні та активні. Пасивний IDS, який виявив зловмисну активність, створюватиме попередження або записи журналу, але не вживає заходів. Активний IDS, який іноді називають системою виявлення та запобігання вторгненням (IDPS), генеруватиме попередження та записи в журналі, але також може бути налаштований на виконання дій, як-от блокування IP-адрес або закриття доступу до обмежених ресурсів.

Системи виявлення вторгнень відстежують мережевий трафік, щоб виявити, коли атака здійснюється неавторизованими особами. IDS роблять це, надаючи деякі (або всі) з наступних функцій фахівцям з безпеки:

– моніторинг роботи маршрутизаторів, брандмауерів, серверів керування ключами та файлів, які необхідні для інших засобів контролю безпеки, спрямованих на виявлення, запобігання або блокування кібератак;
– надання адміністраторам можливості налаштувати, упорядкувати та зрозуміти відповідні журнали аудиту ОС та інші журнали, які інакше важко відстежити або проаналізувати;
– надання зручного інтерфейсу, щоб некваліфіковані співробітники могли допомогти в управлінні безпекою системи;
– включаючи велику базу даних сигнатур атак, з якою можна порівняти інформацію з системи;
– розпізнавання та звітування, коли IDS виявляє, що файли даних були змінені;
– створення повідомлень про порушення безпеки;
– реагування на зловмисників шляхом їх блокування або блокування сервера.

2.4 Переваги та недоліки IDS

Системи виявлення вторгнень пропонують організаціям ряд переваг, починаючи з можливості ідентифікувати інциденти безпеки. IDS можна використовувати для аналізу кількості та типів атак. Організації можуть використовувати цю інформацію, щоб покращити свої системи безпеки або запровадити більш ефективні засоби контролю. Система виявлення вторгнень також може допомогти компаніям виявити помилки або проблеми з конфігурацією мережевих пристроїв. Ці показники потім можна використовувати для оцінки майбутніх ризиків. Системи виявлення вторгнень також можуть допомогти підприємствам досягти відповідності нормативним вимогам. IDS надає компаніям кращу видимість ситуації у своїх мережах,

полегшуючи дотримання правил безпеки. Крім того, підприємства можуть використовувати свої журнали IDS як частину документації, щоб показати, що вони відповідають певним вимогам відповідності. Системи виявлення вторгнень також можуть покращити заходи безпеки. Оскільки датчики IDS можуть виявляти мережеві хости та пристрої, їх також можна використовувати для перевірки даних у мережевих пакетах, а також для ідентифікації ОС послуг, що використовуються. Використання IDS для збору цієї інформації може бути набагато ефективнішим, ніж ручний перепис підключених систем.

IDS схильні до помилкових тривог або помилкових спрацьовувань. Отже, організаціям необхідно налаштувати свої продукти IDS під час їх першого встановлення. Це включає належне налаштування їхніх систем виявлення вторгнень, щоб розпізнати, як виглядає звичайний трафік у їхній мережі порівняно з потенційно шкідливою діяльністю.

Однак, незважаючи на неефективність, яку вони викликають, помилкові спрацьовування зазвичай не завдають серйозної шкоди реальній мережі і просто призводять до покращення конфігурації.

Набагато серйознішою помилкою IDS є ймовірність пропуску загрози і прийняття її за звичний трафік. У хибнонегативному сценарії IT-команди не мають жодних ознак того, що відбувається атака, і часто виявляють це лише після того, як мережа зазнала певного впливу. Для IDS краще бути надмірно чутливим до аномальної поведінки та генерувати хибнопозитивні результати, ніж бути недостатньо чутливим, генеруючи помилкові сповіщення.

Помилкові сповіщення стають все більшою проблемою для IDS, особливо для SIDS, оскільки зловмисне програмне забезпечення розвивається і стає все більш складним. Важко виявити підозрюване вторгнення, оскільки нове зловмисне програмне забезпечення може не відображати раніше виявлені моделі підозрілої поведінки, для виявлення яких зазвичай призначені IDS. Як наслідок, для IDS зростає потреба якнайшвидше виявляти нову поведінку та виявляти нові загрози разом з методами їх уникнення.

2.5 Аналіз існуючих систем

На теперішній час існує багато різних систем виявлення вторгнень але вони мають ряд недоліків.

Однією із таких систем є Wazuh Agent. Wazuh використовується для збору, агрегації, індексації та аналізу даних задля забезпечення безпеки мережі, допомагаючи організаціям виявляти вторгнення, загрози та поведінкові аномалії. Агент забезпечує необхідні можливості моніторингу та реагування, а серверний компонент забезпечує аналіз даних. Агент Wazuh сканує систему, що контролюються, у пошуках шкідливих програм, руткітів та підозрілих аномалій. Він може виявляти приховані файли, приховані процеси або незареєстровані прослуховувачі мережі, а також невідповідності у відповідях на системні виклики.

Wazuh також інтегрований в ELC, що дозволяє використовувати велику кількість інструментів для аналізу, сортування, фільтрування та відображення інформації. Проте для використання цих всіх інструментів необхідно встановлювати клієнт ELC до якого входять Elastic, Logstash, Filebeat та Kibana. Wazuh не є безкоштовним ПЗ і усі дані які він збирає – надсилаються на його сервери для аналізу, це також не є безпечним з точки зору захищеності інформації, адже завжди існує ймовірність компрометації цих даних.

Збір, аналіз, збереження і візуалізацію даних можна забезпечити безпосередньо із використанням тільки ELC, де для збору даних використовується Logstash; для фільтрування, відображення та сортування використовується веб утиліта – Kibana. Але використання цього стеку є невигідним для малої кількості ПК, адже цей стек є досить потужним і націлений на обробку великої кількості інформації не тільки з ПК, а й з комутаторів, маршрутизаторів, фаєрволів та антивірусів.

2.6 Аналіз використаних засобів реалізації власної системи

Головною метою розробки власної системи є втілення всіх доступних можливостей існуючих IDS з найменшим використанням ресурсів ПК.

Я хотів би зосередитись на системі, яка буде автоматично аналізувати log-файли Windows та Unix-подібних системах. Для прикладу ми візьмемо дистрибутив сімейства Linux – Kali Linux встановлений на Virtual Box (Рис. 2.1).

Рисунок 2.1 – Дистрибутив Kali Linux

Доступ до log-файлів в Unix подібних системах ми маємо напряму з командного рядка, всі log-файли знаходяться в директорії /var/log/ (Рис. 2.2). І мають відповідну загальноприйняту структуру (Рис. 2.3).

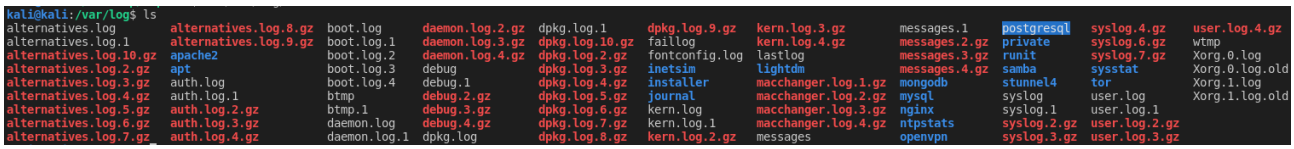

Рисунок 2.2 – Список усіх log-файлів

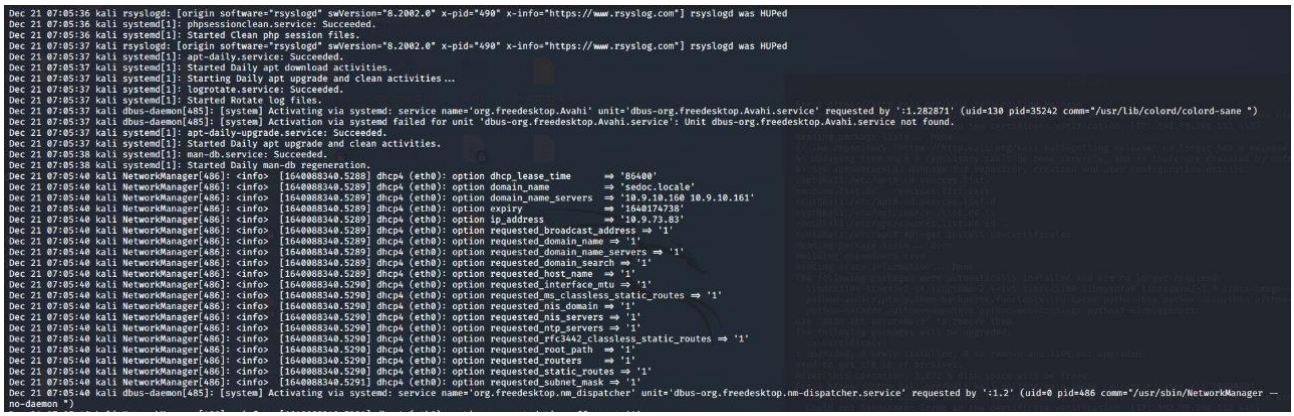

Рисунок 2.3 – Зразок log-файлів Kali Linux

За допомогою Python скріпта ми можемо читати ці файли і аналізувати їх. Також необхідно відокремити важливі дані, які містяться в цих логах, це можливо зробити за допомогою Grok фільтру який є інструментом ELC, а саме цей інструмент використовується в Logstash.

Logstash — це безкоштовний і відкритий конвеєр обробки даних на стороні сервера, який отримує дані з безлічі джерел, перетворює та фільтрує їх, а потім надсилає до сховища. Проте Logstash є дуже ресурсозатратним, і не кожен ПК зможе його використовувати, проте використання фільтра Grok доступне також в Python з використанням відповідної бібліотеки, яка легко встановлюється та має весь потрібний функціонал.

Фільтр Grok дає можливість відфільтрувати та структурувати дані. Log-файли записані у форматі string і мають розширення .log. Grok працює наступним чином: якщо у нас є зразок логу у форматі: “ключ = значення”, він створює для ключа окрему змінну і записує в значення цієї змінної її безпосереднє значення. Для візуального відображення можливих розборів полів використовуються певні сервіси, такі як “Grok Debugger”

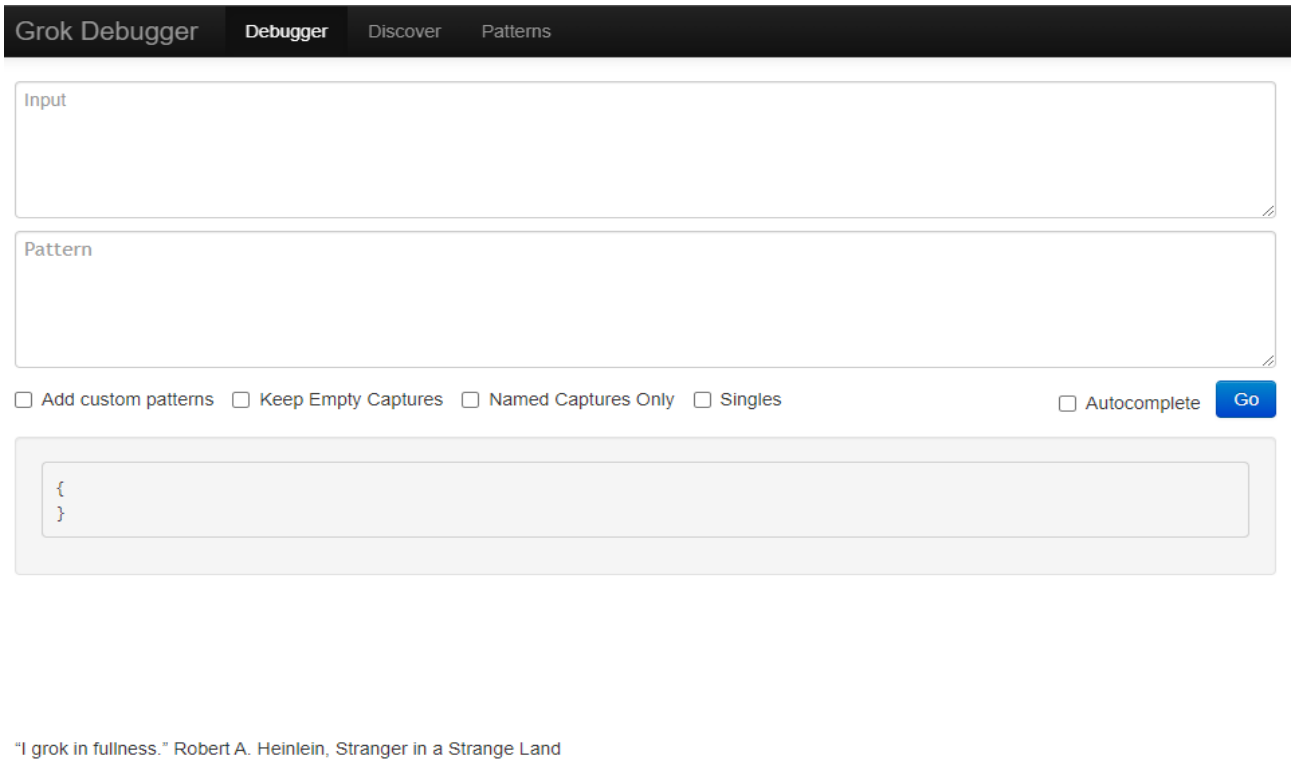

Рисунок 2.4 – Сервіс “Grok Debugger”

Тут ми маємо вхідні дані та патерн, який ми використовуємо для розбиття нашої стрічки яка є частиною log-файлу, в результаті отримуємо уже відфільтровані дані.

Grok дозволяє використовувати власні патерни для визначення типів даних, ці патерни є регулярними виразами і їх приклади також є доступними на сервісі “Grok Debugger” (Рис. 2.5).

```
USERNAME [a-zA-Z0-9._-]+
USER %{USERNAME}
INT (?:[+-]?(?:[0-9]+))
BASE10NUM (?<![0-9.+-])(?>[+-]?(?:(?:[0-9]+(?:\.[0-9]+)?)|(?:\.[0-9]+)))
NUMBER (?:%{BASE10NUM})
BASE16NUM (?<![0-9A-Fa-f])(?:[+-]?(?:0x)?(?:[0-9A-Fa-f]+))
BASE16FLOAT \b(?<![0-9A-Fa-f.])(?:[+-]?(?:0x)?(?:(?:[0-9A-Fa-f]+(?:\.[0-9A-Fa-f]*)?)|(?:\.[0-9A-Fa-f]+)))\b

POSINT \b(?:[1-9][0-9]*)\b
NONNEGINT \b(?:[0-9]+)\b
WORD \b\w+\b
NOTSPACE \S+
SPACE \s*
DATA .*?
GREEDYDATA .*
QUOTEDSTRING (?>(?<!\\)(?>"(?>\\.|[^\\"]+)+"|""|(?>'(?>\\.|[^\\']+)+')|''|(?>`(?>\\.|[^\\`]+)+`)|``))
UUID [A-Fa-f0-9]{8}-(?:[A-Fa-f0-9]{4}-){3}[A-Fa-f0-9]{12}
```

Рисунок 2.5 – Зразок загальновживаних патернів

Для кожного типу даних використовується власний патерн, так для розбору для IP адреси використовується патерн “IP”, проте існують випадки коли в log-файлі може бути або IP адреса або ім’я домену, Grok може опрацювати обидва цих значення за допомогою патерну “IPORHOST” (Рис. 2.6).

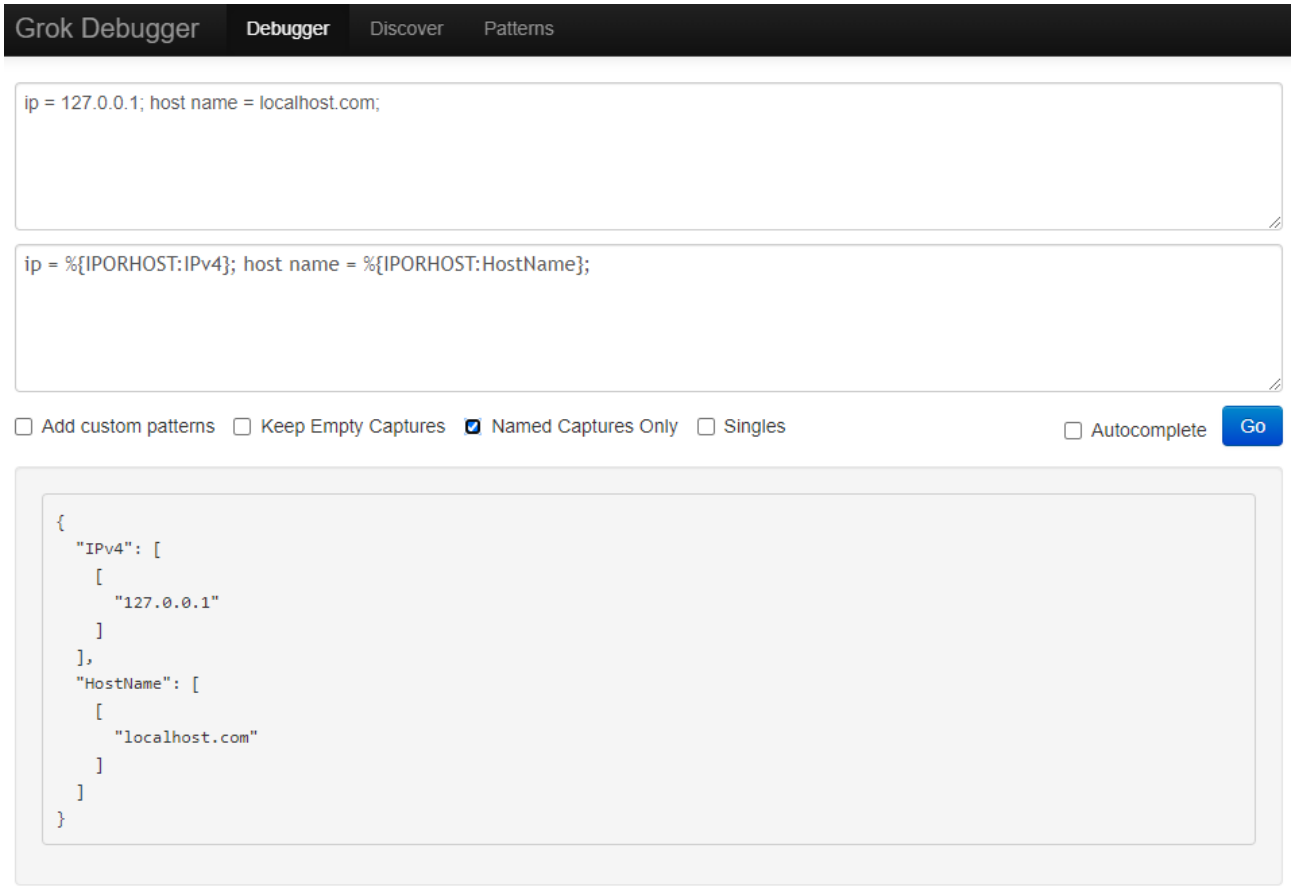

Рисунок 2.6 – Зразок роботи патерну IPORHOST

Так як робота орієнтована на аналіз log-файлів для операційних систем Unix подібних систем та ОС Windows, розглянемо структуру log-файлів також і для Windows ОС. В ОС Windows всі існуючі log-файли можна переглянути за допомогою програми Event Viewer, також Event Viewer дозволяє зберігати log-файли у форматах .txt, .evnt, .csv та .xml (Рис. 2.7).

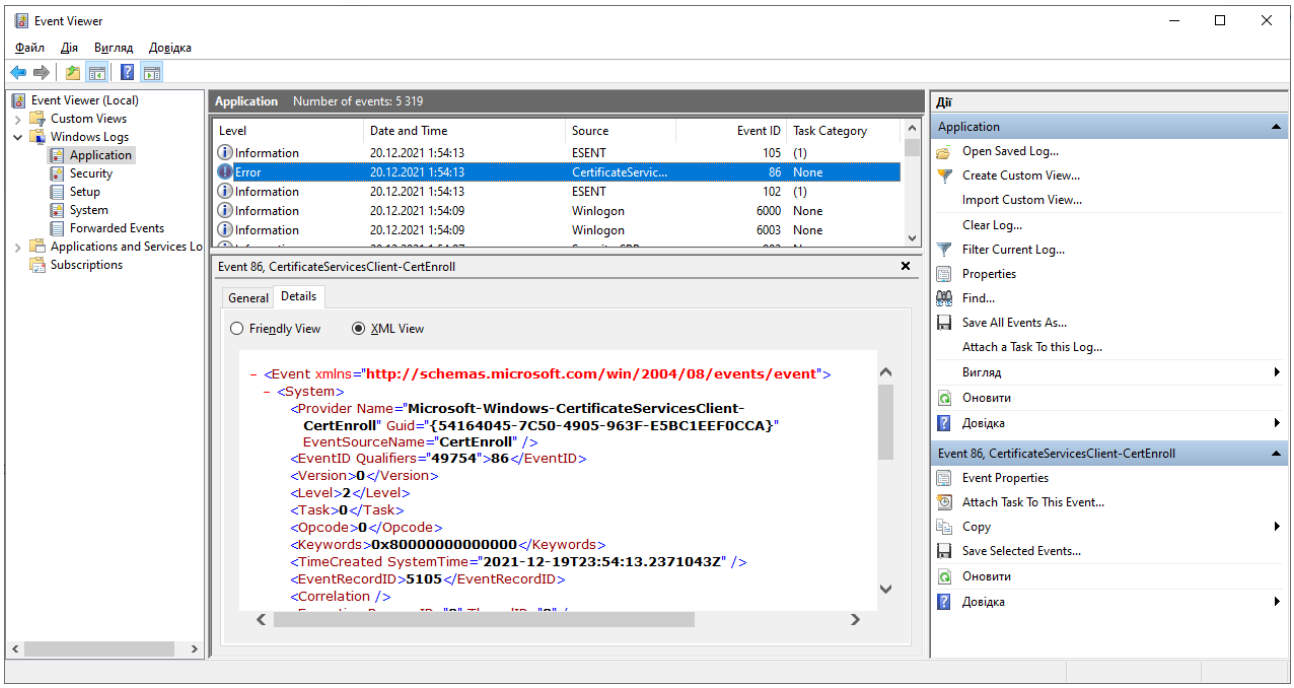

Рисунок 2.7 – Вікно Event Viewer

Для автоматизованого аналізу краще підходить формат .txt, так як з цим форматом зручно працювати використовуючи Python.

Отже, для створення цієї автоматизованої системи рекомендується використовувати наведені вище засоби, тому, що всі вони є у відкритому доступі, та є абсолютно безкоштовними та простими у використанні та налаштуванні. Проте потрібно бути обережним в налаштуванні всіх компонентів системи, адже при найменшій помилці система може працювати некоректно та не зможе забезпечити захист інформації на належному рівні.

3 РОЗРОБКА ТА ТЕСТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

3.1 Реалізація

Обов'язковим кроком перед впровадженням системи моніторингу вторгнень в систему є необхідність перевірити продукт на наявність логічних та граматичних помилок, і перевірити продуктивність. Для цього систему потрібно перевірити в середовищі, для якого вона була розроблена.

Дана структура була застосована до розробки системи автоматично виявлення вторгнень (Рис 3.1). Де кожен елемент відіграє важливу роль у функціонуванні системи.

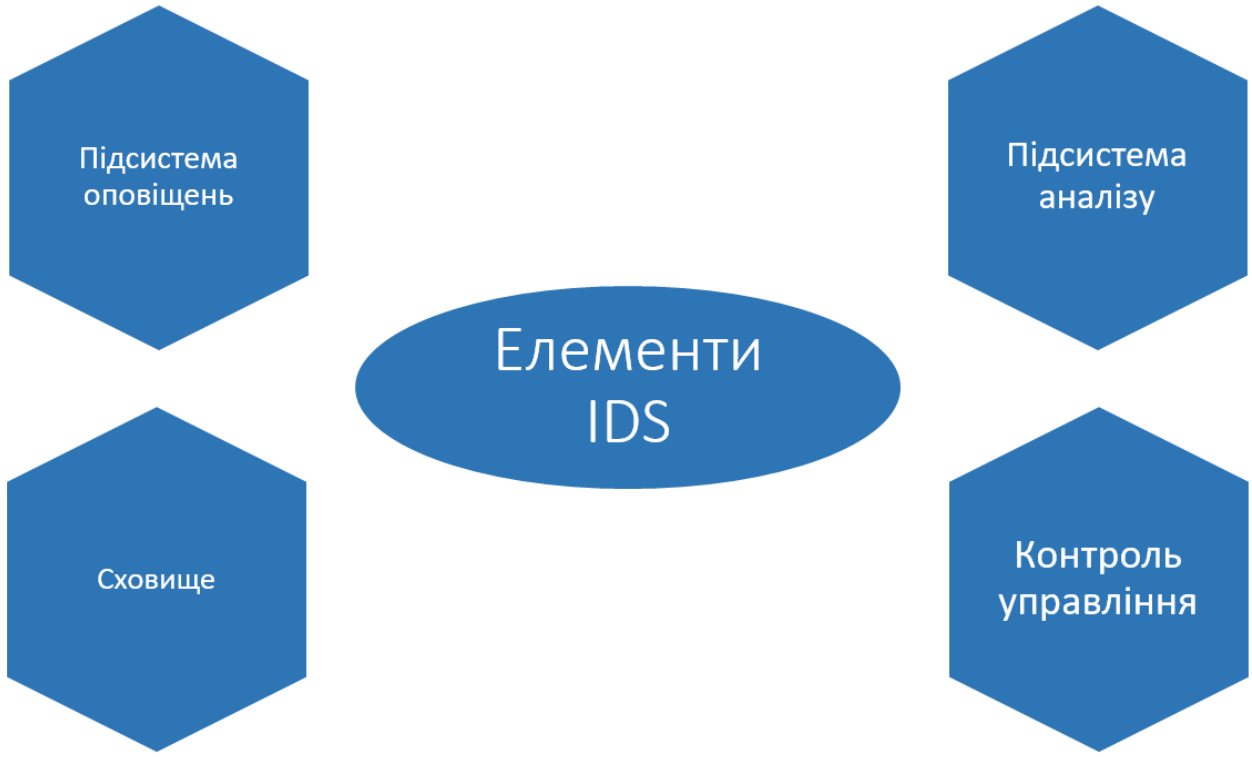

Рисунок 3.1 – Структура IDS системи

Підсистема оповіщень – Накопичує події мережі або комп’ютерної системи.

Підсистема аналізу – Виявлення кібератак та підозрілої активності.

Сховище – Зберігає інформацію про події та результати кібератак, а також несанкціоновані дії.

Контроль управління – Керує параметрами IDS, стежить за станом мережі, дає доступ до інформації про події.

Так як система була розроблена для автоматичного аналізу log-файлів, з метою досягнення найменшого навантаження на систему та отримання належного функціоналу та продуктивності, систему було поділено на кілька частин. Перша частина - клієнтська, це програмний продукт який встановлюється та запускається на ПК клієнта для збору, фільтрування та надсилання логів на сервер. Збір логів здійснюється з допомогою Python скріпта, який читає log-файли, розбиває їх на поля та надсилає на сервер на якому вони зберігаються. Python має свої переваги але також має і недоліки, з переваг це простота синтаксису, гнучкість, єдиний стандарт для написання коду, він дозволяє підтримувати та читати код навіть при переході від одного програміста до іншого, хоч він і не є найбільш продуктивним з поміж інших мов програмування, так як це інтерпретована мова програмування, однак вона допомагає вирішити величезний спектр завдань.

Аналіз та розбиття логів відбувається з допомогою сервісу “Grok Debugger”. Цей же принцип, який зображено на рисунку (Рис. 3.2), використовується і в Python скріпті з використанням бібліотеки pygrok, яка дозволяє розбивати поля на окремі змінні.

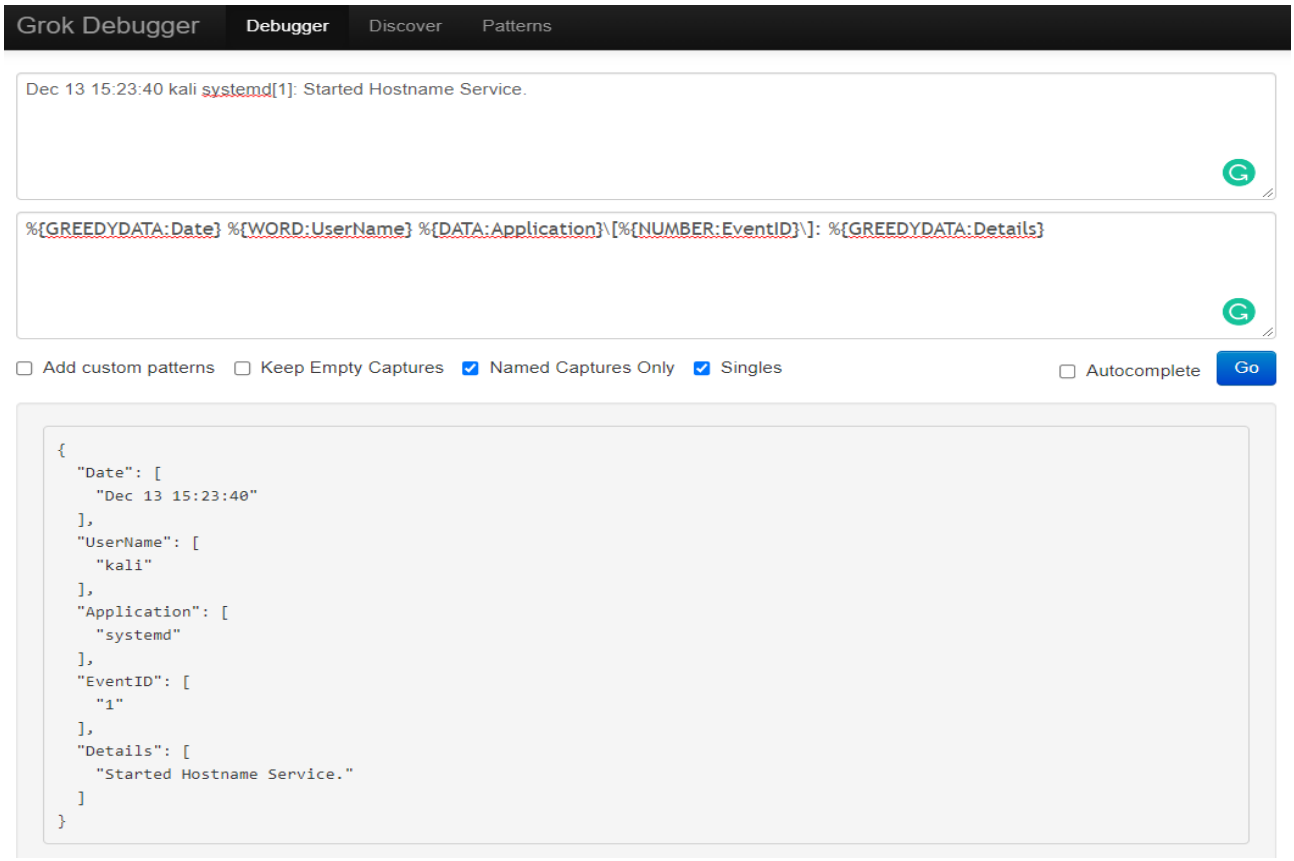

Рисунок 3.2 – Зразок розбору log-файлу в “Grok Debugger”

Бібліотека надзвичайно корисна для використання попередньо створених патернів та аналізу вхідних даних. Патерн для аналізу log-файлів в ОС Kali Linux має наступний вигляд (Лістинг 3.1).

Лістинг 3.1 Функція зі зразком патерну для аналізу log-файлів в ОС Kali Linux

```
    def parsing(lines):
        for line in lines:
            log = str(line)
           pattern = '%{GREEDYDATA:Date} %{WORD:UserName}
%{DATA:ApplicationS}\[%{NUMBER:EventID}\]:
%{GREEDYDATA:Details}'
            grok = Grok(pattern)
            parsed_data = (grok.match(log))
```

Ця функція дозволяє розібрати поле log-файлу за принципом ключ=значення, на вхід подається стрічка а на виході ми маємо структуризовані дані, які надсилаються на сервер.

Як видно на рисунку (Рис. 3.3), вхідні дані було розбито на поля та їх значення, назви полів задаються користувачем вручну.

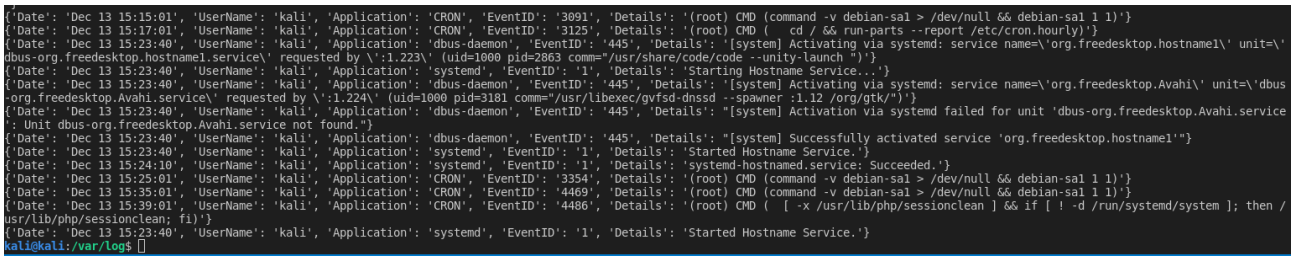

Рисунок 3.3 – Зразок розбору log-файлу за допомогою Python скріпта

Друга частина – серверна. Це місце, де зберігаються усі логи які надійшли від вузлів (клієнтів). Всі журнали подій зберігаються в спеціальних базах даних створених для кожного клієнта або групи клієнтів окремо. Створення окремих баз даних є необхідним, адже потрібно відслідковувати надходження логів, тому структуризація такого типу є альтернативним рішенням. В якості бази даних було використано MongoDB, яка по замовчуванню використовується в Python фреймворку django (Рисунок 3.4). Django – це безкоштовний веб-фреймворк Python, з відкритим вихідним кодом, який слідує архітектурі модель-шаблон.

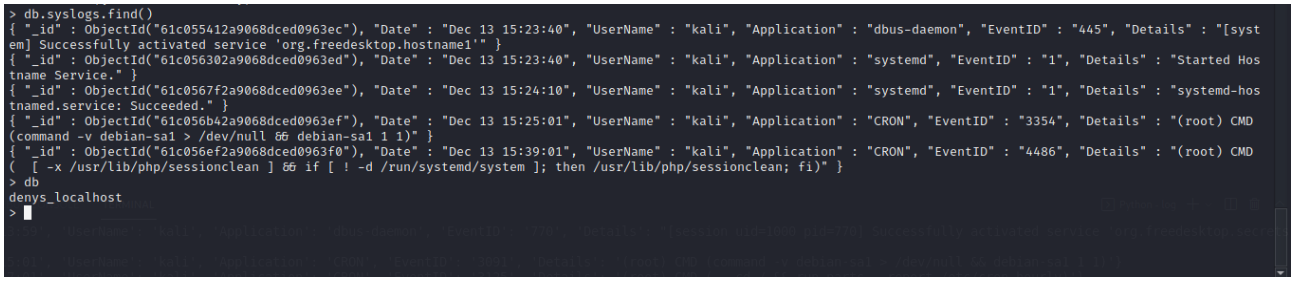

Рисунок 3.4 – Відображення проаналізованих log-файлів в базі даних

Також для зручності спостереження було розроблено панель для візуального відображення всіх логів (Рис. 3.5). Цю панель було створено з використанням фреймворку django. З використанням цієї панелі, адміністратор мережі може відслідковувати всі події, які стаються на вузлах, де є встановлено відповідне ПЗ.

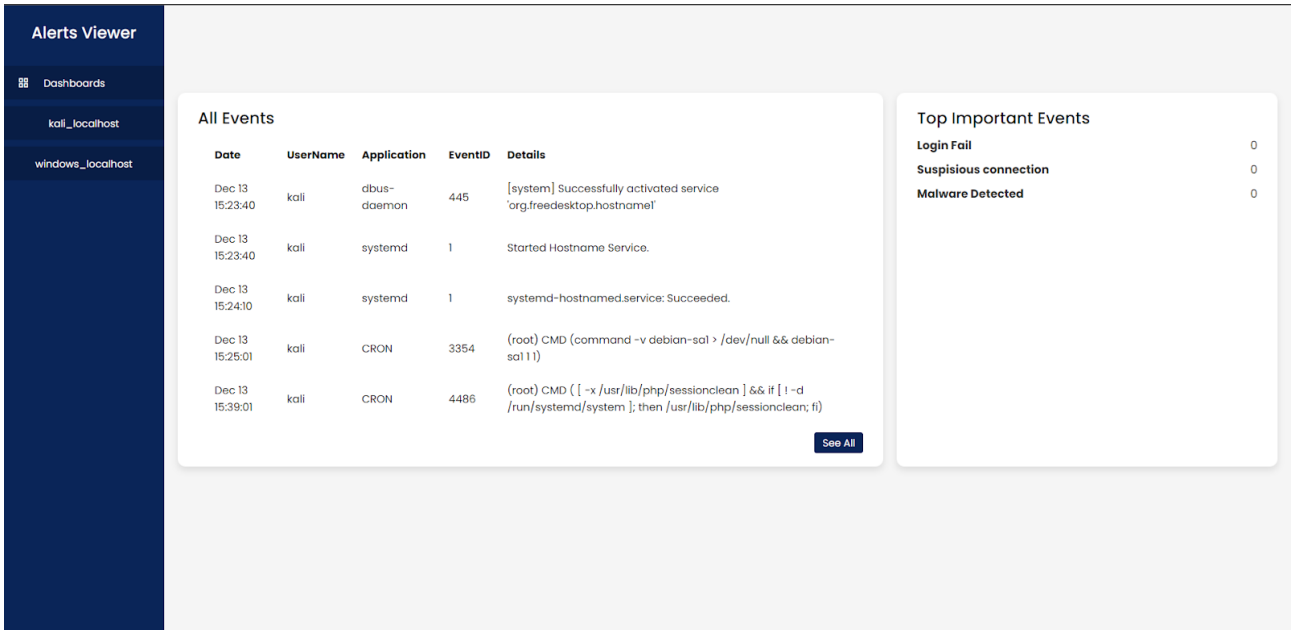

Рисунок 3.5 – Вигляд приладової панелі адміністратора мережі для ОС Kali Linux

Також в Event Viewer існує можливість фільтрації log-файлів за рівнем важливості (Рис. 3.6). Для кращого функціонування системи виявлення вторгнень потрібно визначити які log-файли потребують аналізу, до таких відносяться файли із рівнями: Critical, Error, Verbose та Warning. Тому система виявлення вторгнень аналізувати тільки ці log-файли для швидкодії аналізу і зменшення кількості інформації що записуватиметься до бази даних.

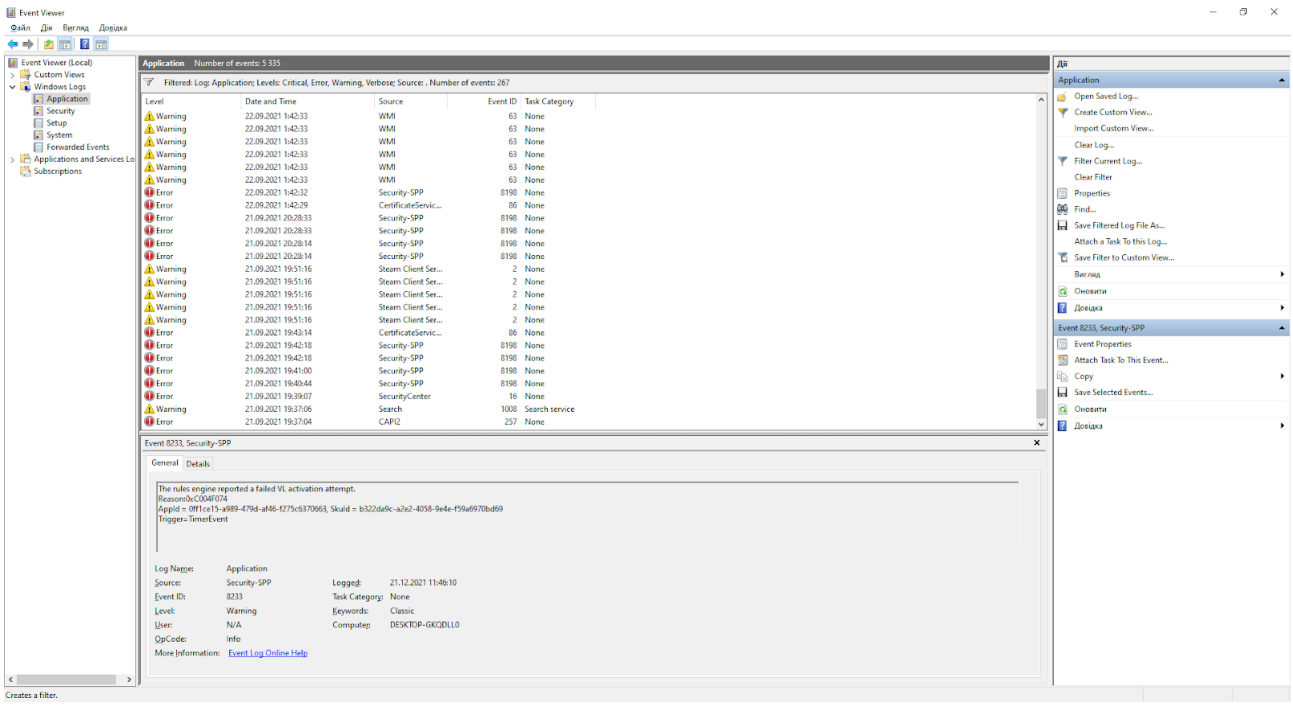

Рисунок 3.6 – Зразок фільтрації log-файлів в Event Viewer

В ОС Windows, log-файли мають іншу структуру ніж в Unix подібних систем, тому для них потрібно створювати окремий патерн для аналізу (Лістинг 3.2).

Лістинг 3.2 Функція зі зразком патерну для аналізу log-файлів в ОС Windows

```
    def parsing(lines):
        for line in lines:
            log = str(line)
            pattern = 'Level=%{DATA:Level} Date and
Time=%{GREEDYDATA:DateAndTime} Source=%{DATA:Source}
Event ID=%{NUMBER:EventID} Task
Category=%{GREEDYDATA:Category}'
            grok = Grok(pattern)
            parsed_data = (grok.match(log))
```

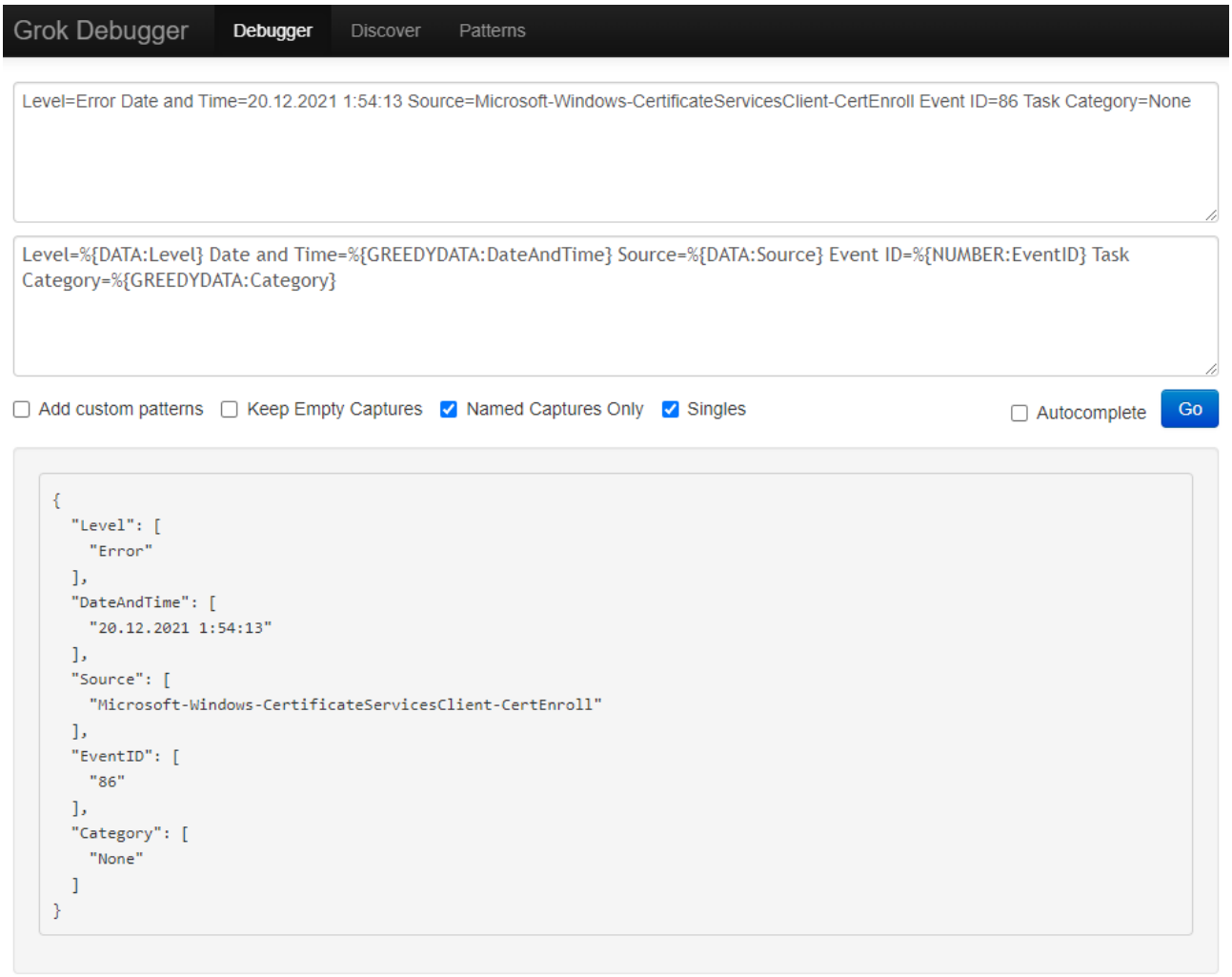

Рисунок 3.7 – Зразок розбору log-файлу ОС Windows в “Grok Debugger”

При аналізі log-файлів вхідна стрічка розбивається на логічні змінні, після чого до цих змінних підбираються відповідні типи патернів, так наприклад для змінної “EventID” підходить патерн %{NUMBER} так як в значенні цієї змінної можуть бути присутні значення тільки в числовому форматі.

Також приладова панель для ОС Windows матиме інший вигляд аніж для Kali Linux (Рис. 3.8).

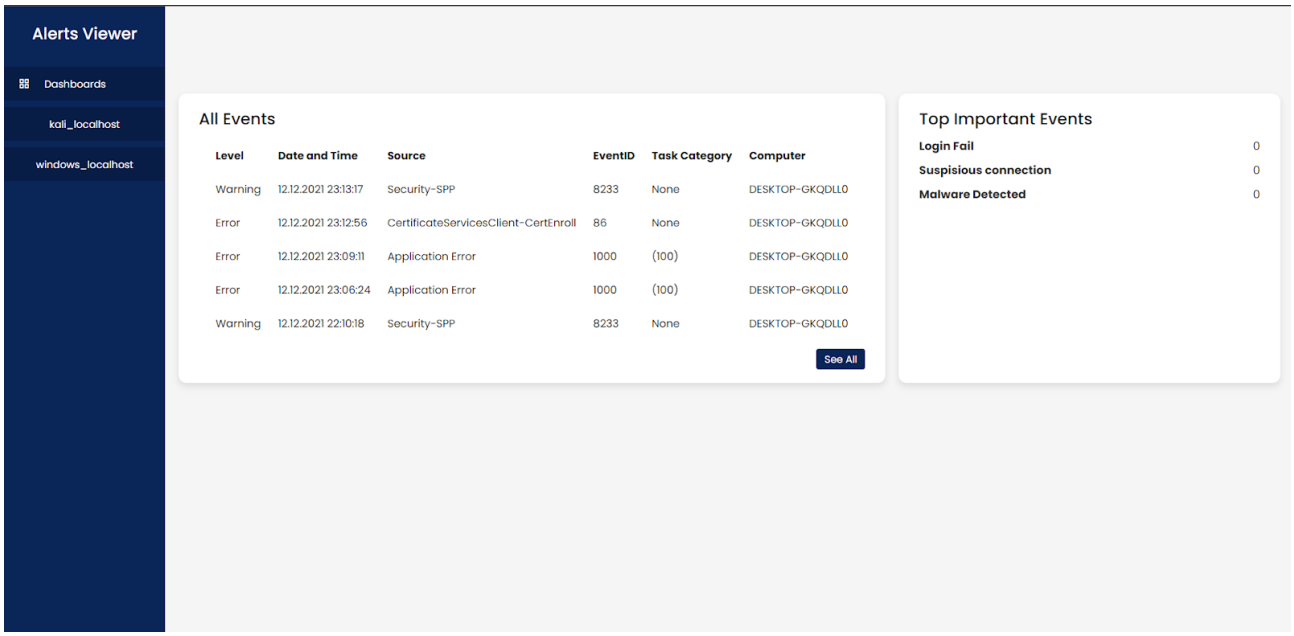

Рисунок 3.8 – Вигляд приладової панелі адміністратора мережі для ОС Windows

3.2 Тестування системи

Для тестування системи потрібно створити подію, яка б порушувала нормальну роботу ОС або яка загрожуватиме безпеці ОС. Для тестування системи було встановлено активатор ОС Windows KMSAuto. При встановлені цього програмного продукту, було створено подію, яка була записана до Event Viewer в розділ /Applications and Services Logs/Microsoft/Windows/Windows Defender/.

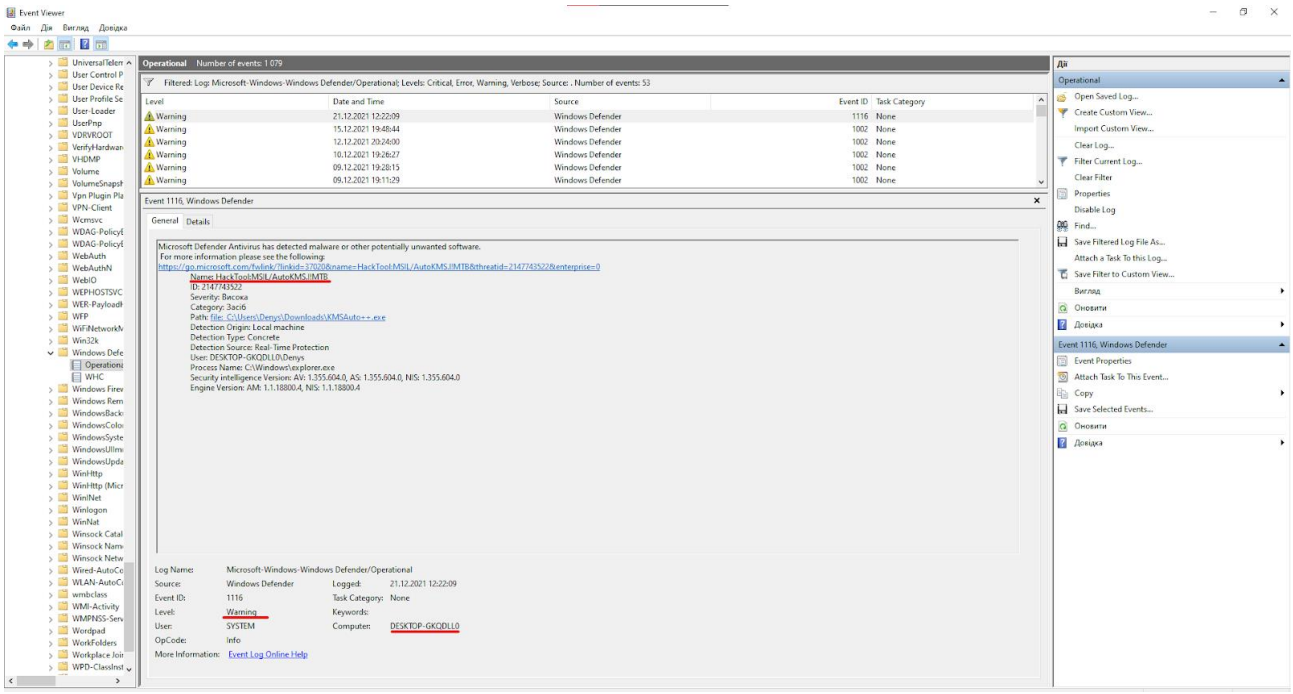

Рисунок 3.9 – Зразок log-файлу з потенційно шкідливим ПЗ в Event Viewer

Windows Defender створив сповіщення про цю подію, вона була проаналізована і виведена до панелі адміністратора. Це

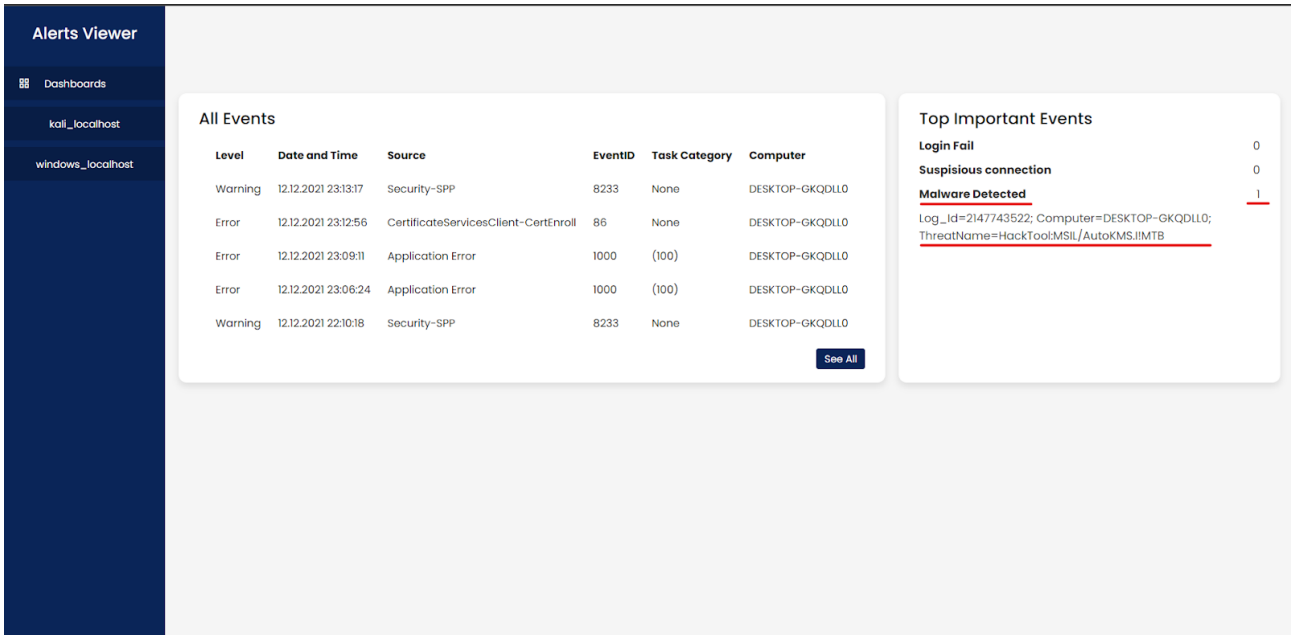

Рисунок 3.10 – Вигляд приладової панелі адміністратора мережі для ОС Windows із відображенням важливої події

3.3 Способи покращення системи виявлення вторгнень

Для покращення роботи цієї системи можливо розширити список джерел надходження log-файлів. Log-файли можуть надсилатися з безлічі різних ресурсів, для прикладу комутатори, маршрутизатори, різного роду ПЗ (антивіруси, програми для аудиту, утиліти). Це дозволить належним чином покращити безпеку мережі в цілому. Також можливо додати візуалізації до панелі адміністратора у вигляді графіків, схем, таблиць та залежностей, для кращого сприйняття та розуміння ситуації, яка виникає в процесі безпосереднього функціонування системи. Можливо також налаштувати певні правила, які базуватимуться на оцінці минулих інцидентів в мережі для того, щоб попередити такі ситуації в майбутньому.

Також можливо додати систему сповіщень з використанням Telegram бота, Teams бота або будь-якого месенджера, який має можливість інтеграції. Ще одним способом надсилання сповіщень є пошта, можливо також реалізувати надсилання важливих подій через корпоративну або будь-яку іншу пошту.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Будь-яке підприємство, установа чи організація, що використовують у своїй діяльності найману працю робітників, повинні передбачити порядок та основні правила взаємодії між підприємством і залученими робітниками. Для цього в компаніях розробляють та затверджують локальні нормативні акти з охорони праці. При підготовці будь-якого документа, а особливо документа з охорони праці, головне — дотриматися юридичних норм та чинного законодавства.

Загалом документи з охорони праці регламентують питання, пов’язані зі збереженням життя, здоров’я і працездатності людини під час трудової діяльності. 2020 рік вніс свої корективи у створення безпечних умов праці та оформлення взаємовідносин між роботодавцем та працівниками. У зв’язку з поширенням COVID-19 та запровадженням в Україні карантину на багатьох підприємствах відбулися зміни в організації роботи. Скорочення, переведення на дистанційну форму роботи, оформлення відпустки за власний рахунок — все це потребує належного документального супроводу.

Закон про охорону праці вимагає від роботодавця одночасно з прийманням працівника на роботу забезпечити йому належні умови праці.

Згідно із ч. 2 ст. 5 Закону про охорону праці під час укладання трудових договорів (крім трудового договору про дистанційну роботу, про роботу вдома) роботодавець повинен поінформувати працівника під розписку про умови праці та наявність на його робочому місці небезпечних і шкідливих виробничих факторів, які ще не усунено, можливі наслідки їх впливу на здоров’я та про права працівника на пільги й компенсації за роботу в таких умовах відповідно до законодавства й колективного договору.

Для виконання обов’язків уповноваженими з питань охорони праці роботодавець за власний рахунок організовує їх навчання, забезпечує

необхідними засобами та звільняє від роботи на передбачений колективним договором строк зі збереженням за ними середнього заробітку (ч. 2 ст. 42 Закону про охорону праці).

Загалом до організації охорони праці входять декілька етапів, а саме:

- атестація робочих місць;
- навчання з охорони праці;
- проведення медоглядів працівників;
- фінансування витрат на охорону праці.

Стисло охарактеризуємо кожен із перелічених вище етапів.

Атестація робочих місць

Порядок її проведення регламентовано Порядком № 442 та Методрекомендаціями № 41.

Відповідно до п. 4 Порядку № 442 атестацію проводить атестаційна комісія, склад і повноваження якої визначають наказом по підприємству, організації, у строки, передбачені колективним договором, але не рідше ніж раз на 5 років.

Позачергово атестацію проводять у разі докорінної зміни умов і характеру праці з ініціативи роботодавця, профспілкового комітету, трудового колективу або його виборного органу, органів Держпраці.

До складу комісії входить уповноважений представник виборного органу первинної профспілкової організації, а за відсутності профспілкової організації — уповноважена найманими працівниками особа.

Результати атестації використовують для розроблення заходів щодо покращення умов праці й оздоровлення працівників та під час визначення права на пенсію за віком на пільгових умовах, пільг і компенсацій за рахунок підприємств, установ та організацій, обґрунтування пропозицій про внесення змін до списків виробництв, робіт, професій, посад і показників, зайнятість у яких надає право на пенсію за віком на пільгових умовах (абз. 1 п. 10 Порядку № 442).

Відповідно до п. 6.9 Методрекомендацій № 41 матеріали атестації робочих місць є документами суворої звітності, та їх зберігають на підприємстві протягом 50 років.

Навчання з охорони праці

Працівники під час прийняття на роботу та в процесі роботи повинні проходити за рахунок роботодавця інструктаж, навчання з питань охорони праці, з надання першої медичної допомоги потерпілим від нещасних випадків і правил поведінки в разі виникнення аварії. Працівники, зайняті на роботах із підвищеною небезпекою чи там, де є потреба в професійному доборі, повинні щороку проходити за рахунок роботодавця спеціальні навчання та перевірку знань відповідних нормативнфо-правових актів з охорони праці (ч.ч. 1, 2 ст. 18 Закону про охорону праці).

Порядок проведення навчання та перевірки знань посадових осіб з питань охорони праці визначений Типовим положенням № 15.

Медогляди працівників

Про обов'язкові медогляди працівників зазначено у ст. 17 Закону про охорону праці. Зокрема, останньою визначено, що роботодавець зобов'язаний за свої кошти забезпечити фінансування й організувати проведення попереднього (під час прийняття на роботу) і періодичних (протягом трудової діяльності) медичних оглядів працівників, зайнятих на важких роботах, роботах зі шкідливими чи небезпечними умовами праці або таких, де є потреба в професійному доборі, щорічного обов'язкового медичного огляду осіб віком до 21 року.

За результатами періодичних медичних оглядів у разі потреби роботодавець повинен забезпечити проведення відповідних оздоровчих заходів.

Медичні огляди проводять відповідні заклади охорони здоров'я, працівники яких несуть відповідальність згідно із законодавством за відповідність медичного висновку фактичному стану здоров'я працівника.

Витрати на забезпечення гігієни та безпеки праці

На роботах зі шкідливими й небезпечними умовами праці, а також роботах, пов’язаних із забрудненням або несприятливими метеорологічними умовами, роботодавець зобов’язаний забезпечити за власний рахунок працівників безоплатно за встановленими нормами спеціальним одягом, спеціальним взуттям та іншими засобами індивідуального захисту, а також мийними та знешкоджувальними засобами (ст. 8 Закону про охорону праці).

4.2 Безпека в надзвичайних ситуаціях

Ефективність економіки держави залежить від того, наскільки окремі галузі господарства здатні стійко працювати не тільки у звичайних умовах, а й в умовах НС мирного та воєнного часу.

Значні руйнування, пожежі та втрати серед населення, викликані наслідками НС, можуть стати причиною різкого скорочення випуску промислової та сільськогосподарської продукції, а отже і зниження економічного потенціалу держави. Виникає потреба завчасного вживання заходів щодо забезпечення стійкої роботи промислових об’єктів на випадок виникнення НС.

Знання можливих НС, характерних для даної місцевості та виробництва, дозволяє диференційовано і цілеспрямовано розробляти та здійснювати заходи, які можуть запобігти аваріям, катастрофам та стихійним лихам або пом’якшити їх наслідки.

Стійкість роботи об’єкта господарської діяльності – це здатність його в умовах НС випускати продукцію у запланованому обсязі та визначеної номенклатури, а у разі слабких та середніх руйнувань або порушення матеріального постачання - відновлювати виробництво власними силами у короткий термін.

На стійкість роботи об’єкта впливають такі фактори:

– захищеність робітників та службовців від уражальних факторів у НС;

– здатність інженерно-технічного комплексу об’єкта (будівель, споруд, обладнання та комунально-енергетичних мереж) протистояти руйнівній дії уражальних факторів аварій, катастроф, стихійного лиха та сучасної зброї;

– надійність постачання об’єкта електроенергією, водою, паливом, комплектуючими та сировиною;

– підготовленість об’єкта до проведення аварійно-рятувальних та відновлюваних робіт;

– оперативність управління виробництвом та здійсненням заходів ЦЗ у НС.

Підвищення стійкості об’єкта досягають проведенням комплексу інженернотехнічних, технологічних, організаційних заходів.

До інженерно-технічних заходів належать роботи, що забезпечують стійкість виробничих будівель і споруд, обладнання та комунально-енергетичних систем.

Технологічні заходи забезпечують підвищення стійкості об’єкта спрощенням технологічного процесу виробництва кінцевої продукції та виключенням або обмеженням розвитку аварій.

Організаційні заходи передбачають розробку ефективних дій керівного складу, служб та формувань ЦЗ, спрямованих на захист виробничого персоналу, проведення рятувальних та інших невідкладних робіт, а також відновлення виробництва.

Основні напрями вкладання фінансових ресурсів на сучасному етапі такі:

– вдосконалення системи моніторингу та прогнозування катастроф і стихійних лих;

– розробка і впровадження функціонального комплексу інформаційного забезпечення процесів управління в НС;

– модернізація автоматизованої системи централізованого оповіщення населення;

– реалізація заходів щодо першочергового життєзабезпечення населення в НС;

– забезпечення населення засобами індивідуального захисту і медикаментами;

– впровадження мобільних комплексів оцінювання стійкості і сейсмостійкості будівель та споруд;

– вдосконалення системи підготовки професійних рятувальників, штатних працівників державних установ у складі спеціально вповноважених органів виконавчої влади з питань ЦЗ, НС та безпеки життєдіяльності об’єктів.

У концепції стійкого розвитку країни передбачено враховувати наслідки реалізації рішень, які приймають в економічній, соціальній, екологічній сферах, і передбачати найповніше оцінювання витрат, вигоди і ризиків за таких критеріїв:

– ніяка господарська діяльність не може бути виправдана, якщо вигода не може покрити збитків, викликаних нею;

– збитки навколишньому середовищу мають бути на найнижчому рівні, який можна розумно досягти з урахуванням економічних і соціальних факторів.

ВИСНОВКИ

Під час виконання даної роботи було опрацьовано багато великий обсяг інформації щодо принципів роботи та способів автоматизованого аналізу даних. Також було проаналізовано переваги та недоліки існуючого ПЗ, яке створено для виявлення несанкціонованих дій в системі.

Ця робота була присвячена розробці автоматизованої системи аналізу log-файлів для виявлення аномальної активності користувача, тому більша частина роботи присвячена тому, як працюють сучасні системи автоматизації, принципи та алгоритми виявлення підозрілої активності, компоненти, які присутні в таких системах, як вони працюють та взаємодіють один з одним. Описано та досліджено методи автоматичного аналізу log-файлів.

При цьому було виконано основне завдання, поставлене для цієї роботи, яке полягало в описі та розробці системи виявлення вторгнень. Його роботу було перевірено в різних середовищах, описані його основні переваги та рекомендації.

Отже, виходячи з усього вищесказаного, можна зробити висновок, що поставлене завдання роботи виконано успішно.

СПИСОК ЛІТЕРАТУРИ

1. M. L. Massie, B. N. Chun, and D. E. Culler, “The ganglia distributed monitoring system: design, implementation, and experience,” Parallel Computing, vol. 30, no. 7, pp. 817 – 840, 2004.
2. Hp insight cluster management utility. URL: http://www8.hp.com/us/en/products/server-software/product-detail.html?oid=3296361.
3. D. Gunter, B. Tierney, K. Jackson, J. Lee, and M. Stoufer, “Dynamic monitoring of high-performance distributed applications,” in High Performance Distributed Computing, 2002. HPDC-11 2002. Proceedings. 11th IEEE International Symposium on, pp. 163–170, 2002.
4. R. Mooney, K. P. Schmidt, and R. S. Studham, “Nwperf: a system wide performance monitoring tool for large linux clusters,” in Cluster Computing, 2004 IEEE International Conference on, pp. 379–389, Sept 2004.
5. M. Kluge, D. Hackenberg, and W. E. Nagel, “Collecting distributed performance data with dataheap: Generating and exploiting a holistic system view,” Procedia Computer Science, vol. 9, pp. 1969 – 1978, 2012. Proceedings of the International Conference on Computational Science, {ICCS} 2012.
6. Ansible. URL: https://www.ansible.com/..
7. Munin. URL: http://munin-monitoring.org/.
8. M/monit. URL: https://mmonit.com/.
9. Collectd. URL: https://collectd.org/.
10. F. D. Sacerdoti, M. J. Katz, M. L. Massie, and D. E. Culler, “Wide area cluster monitoring with ganglia,” in Cluster Computing, 2003. Proceedings. 2003 IEEE International Conference on, pp. 289 – 298, Dec 2003. 41 42 BIB L IO G R A P H Y
11. L. Zhan, T. Z. Fu, D. M. Chiu, and Z. Lei, “A framework for monitoring and measuring a large-scale distributed system in real time,” in Proceedings of the 5th ACM Workshop on HotPlanet, HotPlanet ’13, (New York, NY, USA), pp. 21–26, ACM, 2013.

12. R. Van Renesse, K. P. Birman, and W. Vogels, “Astrolabe: A robust and scalable technology for distributed system monitoring, management, and data mining,” ACM Trans. Comput. Syst., vol. 21, pp. 164–206, May 2003.
13. D. Clough, S. Rivera, M. Kuttel, V. Geddes, and P. Marais, “Panopticon: A scalable monitoring system,” in Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists, SAICSIT ’10, (New York, NY, USA), pp. 39–47, ACM, 2010.
14. J. Joyce, G. Lomow, K. Slind, and B. Unger, “Monitoring distributed systems,” ACM Trans. Comput. Syst., vol. 5, pp. 121–150, Mar. 1987.
15. K. Stefanov, V. Voevodin, S. Zhumatiy, and V. Voevodin, “Dynamically reconfigurable distributed modular monitoring system for supercomputers (dimmon),” Procedia Computer Science, vol. 66, pp. 625 – 634, 2015. 4th International Young Scientist Conference on Computational Science.
16. H. Chen, G. Jiang, C. Ungureanu, and K. Yoshihira, “Combining supervised and unsupervised monitoring for fault detection in distributed computing systems,” in Proceedings of the 2006 ACM Symposium on Applied Computing, SAC ’06, (New York, NY, USA), pp. 705–709, ACM, 2006.
17. L. Tang, T. Li, L. Shwartz, F. Pinel, and G. Y. Grabarnik, “An integrated framework for optimizing automatic monitoring systems in large it infrastructures,” in Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD ’13, (New York, NY, USA), pp. 1249–1257, ACM, 2013.
18. Jsmn. URL: http://zserge.com/jsmn.html.

ДОДАТКИ

М А Т Е Р І А Л И

ІХ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ
2021

УДК 004.056
Д.Ю. Івашин, В.В. Андрушків
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АВТОМАТИЗАІЯ АНАЛІЗУ LOG-ФАЙЛІВ

UDC 004.89
D.Y. Ivashyn, V.V. Andrushkiv

AUTOMATION OF LOG-FILES ANALYSIS

IDS (Intrision Detecion System) – це програмні або апаратні системи, які автоматизують процес перегляду подій, що виникають у комп'ютерній системі чи мережі, аналізують їх з точки зору безпеки. Так як кількість мережевих атак зростає, IDS стають необхідним елементом інфраструктури безпеки. Аналітику кібербезпеки важливо не лише мати цей інструмент в своєму арсеналі, а й розуміти, для яких цілей призначені IDS, як вибрати та налаштувати IDS для конкретних систем і мережевих оточень, як обробляти результати роботи IDS і як інтегрувати IDS з іншою інфраструктурою безпеки підприємства.

Виявлення проникнення є процесом моніторингу подій, що відбуваються в комп'ютерній системі або мережі. Проникнення визначаються як спроби компрометації конфіденційності, цілісності, доступності або обходу механізмів безпеки комп'ютера або мережі. Проникнення можуть здійснюватися як зловмисниками, які отримують доступ до систем з Інтернету, так і авторизованими користувачами систем, що намагаються отримати додаткові привілеї, яких у них немає. Усі події, які відбуваються на персональному комп'ютері (ПК), записуються в спеціальні log-файли, їх ще називають системними файлами, тому що вони містять інформацію про події, які відносяться до програмного забезпечення (ПЗ), безпеки, системи, налаштувань системи, а також час надходження події, її власний ідентифікаційних код та назву виконуваної програми.

IDS володіють функціоналом автоматичного перегляду подій, однак вони, зазвичай, працюють повільно, потребують постійного оновлення даних, не надають детальних даних про події, які виникають в системі, є дуже ресурсо-затратними. Ще однією проблемою є визначення всіх необхідних показників, які можуть бути цінними з точки зору інформаційної безпеки, тому розробка системи, яка може самостійно збирати, систематизувати та аналізувати події на предмет виявлення аномальної поведінки користувача або аномальної мережевої активності є актуальним науковим завданням. [1]

Виявлення проникнення завдяки розпізнаванню аномальної поведінки користувачів чи мережі дозволяє організаціям захищати свої системи від загроз, які пов'язані зі зростанням мережевої активності, запуском підозрілих процесів, великої кількості невдалих авторизацій, відвідуванням фішингових сайтів. В подальшому дослідженні було розроблено систему, яка здатна самостійно опрацьовувати всі події та фільтрувати їх відносно їх пріорітетності та важливості в цілях попередження про загрозу інформаційній безпеці в ОС (операційних системах) Window та Unix-подібних системах.

Проте не варто вважати, що використання IDS та автоматизація аналізу log-файлів дозволить виявити всі загрози безпеки. Кожен засіб захисту адресовано конкретній загрозі безпеки в системі. Більше того, кожен засіб захисту має слабкі та сильні сторони. Тільки правильно підібравши та налаштувавши ці засоби, можна захиститися від максимально великого спектру атак. [2]

Література.

1. What is a Intrision Detecion System. URL: https://www.barracuda.com/glossary/intrusion-detection-system. Last accessed: 27.11.2021
2. IDS usability. URL: https://www.researchgate.net/publication/272476428_CASI_METHOD_FOR_IMPROVING_THE_USABILITY_OF_IDS. Last accessed: 27.11.2021