

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет прикладної математики та інформатики
(повне найменування назва факультету)



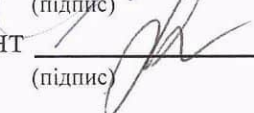
кібербезпеки
(повна назва кафедри)

Дипломна робота

ПОБУДОВА МЕНЕДЖМЕНТУ ВРАЗЛИВОСТЕЙ

Виконав: студент групи ПМК-41с
спеціальності
125 «Кібербезпеки»
(шифр і назва спеціальності)



		Бодьо О. Я.
	(підпис)	(прізвище та ініціали)
Керівник		<u>Бодьо О. Я.</u>
	(підпис)	(прізвище та ініціали)
Рецензент		<u>Клакочевич Л. М.</u>
	(підпис)	(прізвище та ініціали)

Факультет Прикладної математики та інформатики _____

Кафедра Кібербезпеки _____

Спеціальність 125 «Кібербезпека» _____

(шифр і назва)

«ЗАТВЕРДЖУЮ»

Завідувач кафедри _____

"31" серпня 2022 року

ЗАВДАННЯ

НА ДИПЛОМНУ У РОБОТУ СТУДЕНТА

Бодьо Олег Ярославович _____

(прізвище, ім'я, по батькові)

1. Тема роботи Phishing. Розробка програм атаки та захисту.

керівник роботи _____ асистент Карпюк Р.В. _____

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені Вченою радою факультету від " 13" вересня 2022 року № 15 _____

2. Строк подання студентом роботи 13.06.2023р. _____

3. Вихідні дані до роботи отримати дані про вразливості, зробити їх автоматизовану інтеграцію в дата модель Vulnerabilities в SIEM Splunk, візуалізувати дані

4. Зміст дипломної роботи (перелік питань, які потрібно розробити) _____

Теоретичні основи менеджменту вразливостей.

Дослідження менеджменту вразливостей .

Побудова дата моделі та візуалізація даних.

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

Презентація доповіді виконана в Microsoft PowerPoint

6. Консультанти розділів роботи

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

7. Дата видачі завдання 31 серпня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів дипломної роботи	Термін виконання	Примітки
1	Уточнення постановки завдання	21.03.2023	
2	Аналіз літератури	28.03.2023	
3	Обґрунтування вибору рішень	31.03.2023	
4	Збір даних	07.04.2023	
5	Теоретичні відомості	18.04.2023	
6	Дослідження менеджменту вразливостей	20.04.2023	
7	Побудова дата моделі	01.05.2023	
9	Оформлення презентацій	06.06.2023	
10	Отримання рецензій	10.06.2023	
11	Подання роботи на кафедрі	12.06.2023	
12	Захист в ЕК	15.06.2023	

Студент



(підпис)

Бодьо О.Я.
(ініціали, прізвище)

Керівник роботи



(підпис)

Карпюк Р.В.
(ініціали, прізвище)

РЕФЕРАТ

Об'єкт дослідження: інформаційна система, мережа комп'ютерів, програмне забезпечення, апаратне забезпечення або будь-який інший елемент інфраструктури, який може бути піддано аналізу з метою виявлення потенційних вразливостей і застосування заходів щодо їхнього усунення або зменшення ризику їхньої експлуатації.

Метою роботи є забезпечення безпеки інформаційної системи (або іншого об'єкта дослідження) шляхом ідентифікації, оцінки і управління вразливостями. Створення безпечного та стійкого інформаційного середовища, яке захищає важливі дані та ресурси організації від можливих загроз і зловмисного використання.

Галузь застосування. Побудова менеджменту вразливостей є важливою складовою інформаційної безпеки в комп'ютерних системах, мережах і програмному забезпеченні. Вона застосовується у сферах таких як кібербезпека, мережева безпека, захист даних, безпека мобільних пристроїв і т.д.

Ключові слова: Add-on, Data Model, Vulnerability, SIEM.

ABSTRACT

Object of research: an information system, computer network, software, hardware or any other element of the infrastructure that can be subjected to analysis in order to identify potential vulnerabilities and take measures to eliminate them or reduce the risk of their exploitation.

The purpose of the work is to ensure the security of the information system (or other research object) by identifying, assessing and managing vulnerabilities. Creation of a safe and stable information environment that protects important data and resources of the organization from possible threats and malicious use.

Field of application. Building vulnerability management is an important component of information security in computer systems, networks, and software. It is used in areas such as cyber security, network security, data protection, mobile device security, etc.

Keywords: Add-on, Data Model, Vulnerability, SIEM.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ МЕНЕДЖМЕНТУ ВРАЗЛИВОСТЕЙ.....	10
1.1 Nessus.....	10
1.2 SIEM.....	11
1.3 Splunk.....	12
1.4 Дата модель.....	13
Висновки до розділу 1.....	14
РОЗДІЛ 2. ДОСЛІДЖЕННЯ МЕНЕДЖМЕНТУ ВРАЗЛИВОСТЕЙ	15
2.1 Архітектура менеджменту вразливостей.....	15
2.2 Аналіз загроз та визначення основних складових моделі загроз.....	16
2.3 Дослідження Nessus.....	16
2.4 Дослідження SIEM.....	17
2.5 Дослідження Splunk.....	18
2.6 Дослідження дата моделі.....	19
Висновки до розділу 2.....	20
РОЗДІЛ 3. ПОБУДОВА ДАТА МОДЕЛІ ТА ВІЗУАЛІЗАЦІЯ ДАНИХ.....	21
3.1 Технічні відомості.....	21
3.2 Встановлення та отримання даних зі сканера вразливостей Nessus та їх інтеграція в SIEM Splunk.....	21
3.3 Отримання даних.....	21
3.4 Інтеграція даних.....	22
3.5 Передача даних.....	23
3.6 Тегування даних.....	24
3.7 Додавання нового поля до даних.....	24
3.8 Додавання індексу до дата моделі.....	25
3.9 Відсіювання даних з індексу за допомогою нового поля m_tag.....	26
3.10 Адаптація даних зі сканера до дата моделі.....	27
3.11 Додавання полів в дата модель.....	28
3.12 Отримання даних з дата моделі.....	29
3.13 Візуалізація даних.....	29
Висновки до розділу 3.....	31

ВИСНОВКИ.....	32
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	33

ВСТУП

Актуальність. Побудова менеджменту вразливостей залишається надзвичайно актуальною в сучасному світі з наступних причин:

- Зловмисники постійно шукають нові шляхи для злому інформаційних систем, отримання незаконного доступу до даних та спричинення шкоди. Побудова менеджменту вразливостей допомагає ідентифікувати та усувати потенційні слабкі місця в системах, що дозволяє попередити кібератаки.
- Зростання обсягу та значення цифрової інформації. Організації зберігають великі обсяги цінних даних, включаючи конфіденційну інформацію клієнтів, фінансові дані, інтелектуальну власність тощо. Забезпечення безпеки цих даних є критичним завданням, і побудова менеджменту вразливостей є необхідним елементом для захисту цінних активів.
- Законодавчі вимоги та регуляторні стандарти. Багато галузей підлягають специфічним вимогам щодо захисту даних та забезпечення безпеки інформаційних систем. Побудова менеджменту вразливостей допомагає виконувати ці вимоги і забезпечувати відповідність стандартам безпеки.
- Швидкі темпи технологічного розвитку. Постійне впровадження нових технологій, таких як хмарні обчислення, Інтернет речей (IoT) та штучний інтелект, створює нові вразливості і виклики для безпеки. Побудова менеджменту вразливостей дозволяє адаптуватися до змін і забезпечувати безпеку в нових технологічних середовищах.

Метою роботи є забезпечення безпеки інформаційної системи (або іншого об'єкта дослідження) шляхом ідентифікації, оцінки і управління вразливостями. Створення безпечного та стійкого інформаційного середовища, яке захищає важливі дані та ресурси організації від можливих загроз і зловмисного використання.

Для вирішення поставленої мети були сформовані наступні завдання:

- Провести аналіз системи чи об'єкта дослідження з метою виявлення потенційних слабких місць і вразливостей. Це може включати сканування мережі, аудит програмного забезпечення та інші методи дослідження.

- Визначити потенційні наслідки використання вразливостей і оцінити рівень ризику для організації. Це допоможе визначити пріоритети у вирішенні вразливостей та розробці стратегій управління ризиками.
- Розробити і впровадити план дій для усунення або зменшення вразливостей. Це може включати встановлення патчів, оновлення програмного забезпечення, впровадження політик безпеки, навчання персоналу та інші заходи для запобігання використанню вразливостей.
- Постійно контролювати систему, виявляти нові вразливості та перевіряти відповідність стандартам безпеки. Проводити регулярні аудити для перевірки ефективності заходів безпеки та виявлення потенційних проблем.
- Забезпечувати постійне вдосконалення процесів управління вразливістю на основі отриманих даних, аналізу результатів та впровадження нових технологій та методологій. Постійне покращення сприяє ефективному управлінню вразливістю і зменшенню ризиків.

Об'єкт дослідження: інформаційні системи та їхні складові, мережі, фізичні системи, процеси організації.

Предмет дослідження: виявлення, аналіз та управління вразливістю інформаційних систем та їхніх компонентів.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ МЕНЕДЖМЕНТУ ВРАЗЛИВОСТЕЙ

1.1 Nessus

1.1.1 Визначення Nessus. Nessus - це комерційний програмний продукт для сканування вразливостей та оцінки безпеки комп'ютерних систем. Він використовується для виявлення потенційних слабких місць, налаштування безпеки та оцінки ризиків у мережах і інформаційних системах. Nessus надає можливість проводити активне сканування для виявлення вразливостей у різних компонентах системи, включаючи операційні системи, додатки, мережеві пристрої та інші. Результати сканування надаються у зрозумілому форматі, що дозволяє аналізувати та вживати відповідних заходів для забезпечення безпеки і захисту інформаційних систем.

1.1.2 Переваги Nessus:

- Широке охоплення вразливостей: Nessus має велику базу даних з оновленнями і відомими вразливостями, що дозволяє здійснювати детальне сканування системи і виявляти широкий спектр потенційних проблем безпеки.
- Гнучкість та налаштування: Програмне забезпечення Nessus надає користувачам можливість настроїти сканування під свої потреби. Це дозволяє враховувати специфічні характеристики мережі та системи, щоб отримати більш точні результати.
- Розширені звіти та аналіз: Nessus надає детальні звіти та аналіз результатів сканування. Це допомагає зрозуміти знайдені вразливості, їхні потенційні наслідки та рекомендації щодо вирішення проблем безпеки.
- Підтримка різних платформ: Nessus підтримує сканування різних операційних систем, додатків та мережевих пристроїв, що дозволяє охопити широкий спектр інфраструктури й аналізувати потенційні вразливості.
- Підтримка великих мереж: Nessus може бути використаний для сканування великих мереж з великою кількістю систем і пристроїв, надаючи зручні інструменти для управління та моніторингу безпеки в розмаїтих середовищах.

1.1.3 Результати сканування Nessus надаються у вигляді детальних звітів, які містять інформацію про виявлені вразливості, їх серйозність, можливі

наслідки та рекомендації щодо усунення проблем. Звіти можуть містити таку інформацію:

- Виявлені вразливості: Список знайдених вразливостей, включаючи їх назву, опис та рівень серйозності. Це можуть бути слабкі місця в операційній системі, програмному забезпеченні або конфігураційні проблеми.
- Рівень серйозності: Класифікація вразливостей за рівнем серйозності, наприклад, критичні, високі, середні або низькі, враховуючи потенційний вплив на систему та можливість зловживання.
- Рекомендації щодо вирішення: Наведення рекомендацій та керівництва щодо усунення виявлених вразливостей, включаючи встановлення патчів, налаштування захисту, зміну конфігурації або інші кроки для запобігання можливим атакам.
- Інформація про активи: Інформація про скановані активи, такі як IP-адреси, порти, системи, що виявлені, інформація про оперативну систему та інші деталі.
- Додаткові дані: Звіти можуть містити додаткову інформацію про сканування, таку як час проведення, налаштування сканування, результати політик безпеки та інші параметри.
- Звіти Nessus надають зрозумілу інформацію для аналізу виявлених вразливостей та вживання відповідних заходів для забезпечення безпеки системи.

1.2 SIEM

1.2.1 SIEM (Security Information and Event Management) - це комплексна система, яка поєднує в собі рішення з управління інформаційною безпекою та подіями. SIEM забезпечує збір, аналіз та інтерпретацію інформації про події, які відбуваються в комп'ютерних системах та мережах.

1.2.2 Основні функції SIEM включають:

- Збір журналів подій: SIEM здатний збирати, агрегувати та зберігати журнали подій з різних джерел, таких як сервери, роутери, фаєрволи, антивірусні програми тощо.
- Кореляція подій: SIEM аналізує зібрані дані та застосовує розуміння контексту для виявлення взаємозв'язків між подіями, що можуть вказувати на потенційну кіберзагрозу або інцидент безпеки.
- Виявлення загроз: SIEM використовує правила, алгоритми та аналітику для виявлення незвичайної або підозрілої активності в

системі. Це може включати виявлення атак, вторгнень, витоку даних та інших загроз безпеці.

- Сповіщення та реагування: SIEM надає можливість генерувати сповіщення або відправляти тривожні повідомлення у разі виявлення підозрілої або шкідливої активності. Крім того, SIEM може надавати інформацію для подальшого розслідування та відновлення після інциденту.
- Архівування та аудит: SIEM забезпечує можливість зберігати журнали подій на тривалий термін, що дозволяє проводити аудит та аналіз минулих подій для виявлення трендів або встановлення відповідності вимогам Міжнародних стандартів безпеки, таких як PCI DSS, HIPAA, GDPR тощо.

1.2.3 Використання SIEM.

SIEM може використовуватися для моніторингу та управління безпекою в реальному часі, виявлення і реагування на загрози, включаючи атаки ззовні та внутрішні порушення безпеки. Він також може допомагати в розслідуванні інцидентів, аналізувати дані для виявлення потенційних вразливостей та ризиків, а також сприяти впровадженню найкращих практик у сфері інформаційної безпеки.

1.2.4 Інтеграція SIEM.

SIEM може бути інтегрований з іншими системами безпеки, такими як системи виявлення вторгнень (IDS) або системи управління подіями в області безпеки (Security Event Management - SEM), щоб забезпечити комплексний підхід до безпеки та виявлення інцидентів.

1.3 Splunk

1.3.1 Splunk - це платформа для опрацювання та аналізу великого обсягу даних (Big Data), яка спеціалізується на зборі, індексуванні, пошуку, візуалізації та аналізі машинних даних з різних джерел.

1.3.2 Основною сутністю Splunk є розподілена система обробки даних, яка може збирати дані з різних джерел, таких як серверні журнали, мережеві пристрої, додатки, сенсори IoT та інші. Splunk індексує ці дані, що дозволяє швидко здійснювати пошук, фільтрацію та аналіз даних у реальному часі.

1.3.3 Застосування Splunk.

Splunk знаходить широке застосування в області моніторингу систем, безпеки, логістики, аналітики веб-серверів та додатків, аналізу маркетингових даних, виявлення аномалій, прогнозування та багатьох інших галузях. Він може допомогти організаціям виявляти проблеми, аналізувати тренди, забезпечувати безпеку та приймати обґрунтовані рішення на основі великого обсягу даних.

1.4 Дата модель

1.4.1 Дата модель - це абстрактне відображення реальної системи або домену, яке використовується для опису структури даних, їх взаємозв'язків та правил обробки. Модель даних допомагає організувати та розуміти дані в контексті конкретної системи, додатку або предметної області.

1.4.2 Представлення дата моделі.

Модель даних може бути представлена у вигляді діаграми, текстового опису або комбінації обох. Вона описує сутності (entities), атрибути (attributes) та відношення (relationships) між ними. Модель даних може також включати правила цілісності (integrity constraints), обмеження (constraints) та інші властивості, що регулюють дані.

1.4.3 Типи дата моделей включають:

- Ієрархічну дата модель (Hierarchical Data Model): дані представлені у вигляді деревоподібної ієрархії, де кожен запис має одного батька і може мати декількох дітей.
- Мережеву дата модель (Network Data Model): дані представлені у вигляді мережі, де записи можуть мати кілька батьків і дітей, утворюючи складні зв'язки.
- Реляційну дата модель (Relational Data Model): дані представлені у вигляді таблиць, де існують відношення між таблицями, використовуючи ключі.
- Об'єктно-орієнтовану дата модель (Object-Oriented Data Model): дані представлені у вигляді об'єктів з властивостями та методами, що описують їх поведінку.
- Інші моделі, такі як схема зіставлення (schema mapping), модель ключ-значення (key-value model), графова модель (graph model) та інші.

Висновки до розділу 1.

Nessus, SIEM (Security Information and Event Management), Splunk та модель даних є важливими елементами сфери безпеки та обробки даних.

Nessus - це інструмент для сканування вразливостей, який допомагає виявляти потенційні проблеми з безпекою. Використання Nessus дозволяє організаціям ідентифікувати слабкі місця та приймати заходи для виправлення вразливостей.

SIEM є комплексною системою моніторингу та управління безпекою, яка збирає, аналізує та реагує на події з різних джерел. SIEM допомагає виявляти загрози безпеки, розслідувати інциденти та забезпечувати впровадження найкращих практик у сфері інформаційної безпеки.

Splunk - це потужна платформа для обробки та аналізу великого обсягу даних. Використовуючи Splunk, можна здійснювати збір, індексацію, пошук, аналіз та візуалізацію даних з різних джерел. Splunk допомагає організаціям отримувати глибокий аналіз даних та зрозуміти їх в контексті системи або додатку.

Дата модель - це абстрактне відображення структури даних та їх взаємозв'язків. Вона допомагає організувати та розуміти дані в рамках конкретної системи або предметної області. Різні типи дата моделей (ієрархічна, мережева, реляційна, об'єктно-орієнтована) використовуються для структурування та розуміння даних залежно від потреб та контексту.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ МЕНЕДЖМЕНТУ ВРАЗЛИВОСТЕЙ

2.1 Архітектура менеджменту вразливостей включає наступні ключові компоненти:

- Сканування вразливостей: Цей компонент використовує спеціальні інструменти, такі як Nessus, для сканування системи та виявлення вразливостей. Він перевіряє конфігурацію системи, наявність патчів та інші потенційні слабкі місця.
- Оцінка ризиків: Після виявлення вразливостей проводиться оцінка їх ризиків. Це включає аналіз потенційних наслідків вразливостей, ймовірності їх використання зловмисниками та впливу на систему.
- Планування заходів: На основі оцінки ризиків формується план заходів для вирішення вразливостей. Це можуть бути встановлення патчів, зміни конфігурації, розробка політик безпеки та інші заходи для зменшення ризиків.
- Впровадження заходів: Після планування заходів реалізується їх впровадження. Це включає встановлення патчів, налаштування системи, впровадження політик безпеки та інші кроки для забезпечення безпеки системи.
- Моніторинг та аналіз: Після впровадження заходів важливо здійснювати постійний моніторинг стану системи та аналізувати вразливості, які можуть виникати з часом. Це дозволяє вчасно реагувати на нові загрози та забезпечувати постійний рівень безпеки.
- Консолідація та звітність: Цей компонент відповідає за збір інформації про вразливості, заходи безпеки та їх впровадження з різних джерел і систем. Він забезпечує консолідацію даних і формування звітів, що дозволяє керівництву та експертам з безпеки отримати об'єктивну інформацію про стан безпеки системи.
- Неперервність бізнесу: В архітектурі менеджменту вразливостей важливо враховувати аспекти неперервності бізнесу. Це означає розробку планів реагування на інциденти, резервне копіювання даних, відновлення систем та інші заходи для забезпечення стійкості бізнес-процесів навіть при вразливостях та атаках.
- Інтеграція з існуючими системами: Архітектура повинна бути здатною інтегруватися з існуючими системами у компанії, такими як системи моніторингу, інцидентного керування та автоматизовані системи керування безпекою. Це сприяє ефективному обміну даними та покращує синергію між різними компонентами безпеки.

- Комунікація та співпраця: Важливим елементом архітектури є забезпечення ефективної комунікації та співпраці між різними зацікавленими сторонами, такими як відділи безпеки, ІТ-відділ, керівництво компанії та постачальники. Це дозволяє швидше реагувати на вразливості та приймати належні рішення для забезпечення безпеки.

2.2 Аналіз загроз та визначення основних складових моделі загроз є важливою частиною процесу управління ризиками та безпекою. Для цього використовуються такі етапи:

- Ідентифікація загроз: Визначення потенційних загроз, які можуть вплинути на систему або організацію. Це можуть бути такі загрози, як хакерські атаки, віруси, фішинг, природні катастрофи тощо.
- Аналіз загроз: Вивчення та оцінка кожної загрози, включаючи її характеристики, потенційний вплив, ймовірність виникнення та наслідки. Це допомагає визначити пріоритети та вагомість кожної загрози.
- Визначення цілей: Встановлення цілей безпеки та ризикового менеджменту, які необхідно досягти для захисту від загроз. Ці цілі повинні бути конкретними, вимірними, досяжними, релевантними та часово обмеженими.
- Визначення складових моделі загроз: Розбиття загроз на основні складові елементи або категорії. Це можуть бути такі складові, як технічні загрози, організаційні загрози, природні загрози, людські загрози тощо. Кожна складова може мати свої власні характеристики та специфіку.
- Оцінка ризиків: Визначення рівня ризику для кожної загрози на основі її ймовірності виникнення та потенційного впливу. Це допомагає встановити пріоритетність заходів безпеки та ресурси, які слід спрямовувати на зменшення ризиків.

2.3 Дослідження Nessus.

Основна мета дослідження Nessus полягає у виявленні потенційних загроз безпеці, що можуть бути використані зловмисниками для злому або зловживання системою.

Дослідження Nessus може включати наступні кроки:

- Конфігурація та підготовка: Цей крок включає налаштування Nessus для сканування системи або мережі, вибір типів сканування та визначення параметрів, таких як обсяг сканування та періодичність.

- Виконання сканування: Після налаштування Nessus запускається процес сканування, під час якого Nessus автоматично перевіряє систему на наявність вразливостей. Він може проводити сканування портів, служб, додатків та інших складових системи.
- Аналіз результатів: Після завершення сканування Nessus генерує звіт, що містить результати сканування та виявленні вразливості. Дослідник безпеки аналізує ці результати для ідентифікації потенційних проблем та оцінки їх важливості.
- Виправлення вразливостей: На основі результатів дослідження Nessus, організація приймає заходи для виправлення виявлених вразливостей. Це може включати встановлення патчів, зміну конфігурації системи або впровадження інших заходів безпеки.
- Перевірка після виправлення: Після виправлення вразливостей проводиться повторне сканування за допомогою Nessus для перевірки ефективності вжитих заходів безпеки та запевнення у відсутності нових вразливостей. Перевірка допомагає встановити, чи були всі проблеми вирішені і чи вдалося забезпечити безпеку системи або мережі.
- Постійний моніторинг безпеки: Оскільки загрози безпеки постійно змінюються, дослідження Nessus є процесом, який слід проводити регулярно. Постійний моніторинг безпеки дозволяє виявляти нові вразливості, виконувати оновлення та вживати необхідні заходи безпеки для збереження надійності системи.

2.4 Дослідження SIEM.

Основна мета дослідження SIEM полягає у зборі, аналізі та реагуванні на події безпеки з різних джерел, забезпечуючи цілісну картину безпекового стану організації.

Дослідження SIEM може включати наступні етапи:

- Конфігурація та налаштування: Цей крок включає налаштування SIEM для збору та аналізу журналів подій з різних джерел, таких як фаєрволи, системи виявлення вторгнень, сервери та інші. Налаштування також включає визначення правил та політик безпеки для спостереження за підозрілими активностями.
- Збір та аналіз подій: SIEM збирає, індексує та аналізує події безпеки з різних джерел. Це можуть бути спроби несанкціонованого доступу, аномальні активності, виявлення вразливостей тощо. Аналіз подій включає виявлення загроз, розпізнавання зразків та специфічних сценаріїв атак.
- Реагування на події: На основі аналізу подій SIEM сповіщає про потенційні загрози та інциденти безпеки. Це може включати автоматичне сповіщення,

вироблення детальних звітів, виклик експертів з безпеки або автоматичну відповідь на загрози.

- Аудит та відстеження: SIEM дозволяє вести аудит та відстеження подій, що відбуваються в системі. Це допомагає виявляти порушення політик безпеки, аналізувати причини інцидентів та приймати заходи для запобігання подібним інцидентам у майбутньому. Аудит та відстеження допомагають забезпечити дотримання норм безпеки і розкриття потенційних слабких місць в системі.
- Постійне вдосконалення: Дослідження SIEM включає постійний аналіз та вдосконалення системи. На основі результатів аналізу подій та виявлених вразливостей, організація може приймати заходи для покращення політик безпеки, впровадження нових правил та розробки стратегій протидії загрозам безпеки.
- Забезпечення відповідності: SIEM також може використовуватися для забезпечення відповідності з регуляторними вимогами та стандартами безпеки. Дослідження SIEM допомагає виявляти та документувати відповідність організації вимогам щодо збереження даних, доступу та безпеки.

2.5 Дослідження Splunk.

Основна мета дослідження Splunk полягає у зборі, індексації, аналізі та візуалізації даних з різних джерел для підтримки прийняття рішень, виявлення аномалій та вирішення проблем.

Дослідження Splunk може включати наступні етапи:

- Конфігурація та збір даних: Цей крок включає налаштування Splunk для збору даних з різних джерел, таких як лог-файли, бази даних, сенсори IoT та інші. Дані можуть бути структурованими або неструктурованими. Splunk забезпечує механізми для ефективного збору та індексування даних.
- Аналіз та витягування інформації: Після збору даних Splunk надає можливість для аналізу та витягування цінної інформації з них. Це може включати пошук та фільтрацію даних, застосування аналітичних методів, створення запитів та створення звітів.
- Візуалізація та звіти: Splunk дозволяє створювати візуалізації та звіти на основі аналізованих даних. Це дозволяє легко сприймати та розуміти отримані результати. Візуалізація може бути у вигляді графіків, діаграм, теплових карт та інших форматів.
- Моніторинг та оповіщення: Splunk надає можливість постійного моніторингу стану системи та даних. Він може надсилати сповіщення в

реальному часі про виявлені проблеми, загрози безпеки або незвичайні активності. Це дозволяє оперативно реагувати на події та забезпечувати безпеку та ефективність системи.

- Постійне вдосконалення: Дослідження Splunk є неперервним процесом, який дозволяє вдосконалювати аналітичні методи, засоби візуалізації та розширювати функціональні можливості. Організація може вдосконалювати свої аналітичні здібності, налаштовувати звіти та панелі управління відповідно до змінних потреб та вимог.

2.6 Дослідження даних моделі.

Основна мета дослідження моделі даних полягає в аналізі, документуванні та вдосконаленні способу представлення даних, що використовується в системі.

Дослідження моделі даних може включати наступні етапи:

- Аналіз потреб: Перший крок у дослідженні моделі даних - аналіз потреб організації щодо даних. Це включає виявлення основних сутностей, атрибутів та зв'язків, які необхідні для ефективного управління даними в організації.
- Проектування моделі: На основі аналізу потреб визначається структура та зв'язки між різними сутностями та атрибутами. Модель даних може бути представлена у вигляді схеми, діаграми або іншого графічного формату, який відображає структуру даних.
- Валідація та оптимізація: Після проектування моделі важливо перевірити її на відповідність потребам організації та правильність структури. Виявлені недоліки можуть бути виправлені, а модель даних може бути оптимізована для поліпшення продуктивності та ефективності роботи з даними.
- Аналіз та використання: Після документування моделі даних, її можна використовувати для різних цілей. Це може включати розробку баз даних, реалізацію систем управління базами даних, розробку програмного забезпечення або створення аналітичних звітів. Модель даних використовується як основа для розробки та розширення функціональності системи.
- Вдосконалення та розвиток: Дослідження моделі даних є неперервним процесом. З розвитком організації та зміною потреб змінюються й вимоги до моделі даних. Тому важливо вдосконалювати модель, вносячи необхідні зміни та адаптації, щоб вона відповідала новим вимогам та стандартам.

Висновки до розділу 2.

Дослідження Nessus, SIEM, Splunk та моделі даних є важливими етапами в розробці, впровадженні та управлінні інформаційною безпекою та даними в організаціях.

Nessus є потужним інструментом для виявлення вразливостей та аналізу безпеки систем. Він надає широкий набір функцій для сканування мережі, аудиту систем та виявлення потенційних загроз безпеці. Дослідження Nessus дозволяє організаціям підвищити рівень безпеки своїх систем та даних.

SIEM є комплексною системою, яка забезпечує централізоване керування та моніторинг подій в мережі. Він дозволяє виявляти та реагувати на безпекові події в реальному часі, забезпечуючи високий рівень безпеки та детективність. Дослідження SIEM допомагає організаціям побудувати ефективну систему безпеки, виявляти загрози та реагувати на них швидко і ефективно.

Splunk є потужною платформою для аналізу та використання даних з різних джерел. Він надає можливості для виявлення аномалій, моніторингу та оповіщення про події, аналітики даних та постійного вдосконалення. Дослідження Splunk дозволяє організаціям отримати цінні інсайти з даних, забезпечити безпеку та ефективність системи.

Дослідження моделі даних також допомагає забезпечити якість даних шляхом визначення правил валідації, обмежень та способів зберігання даних. Це дозволяє уникнути помилок, дублікатів та некоректних даних, що можуть негативно вплинути на прийняття рішень та ефективність роботи організації.

Дослідження моделі даних є ключовим етапом при розробці нових систем, внесенні змін до існуючих систем або інтеграції різних джерел даних. Воно допомагає зрозуміти потреби користувачів, вимоги до функціональності та зв'язки між різними частинами системи. Це сприяє розробці ефективних рішень, що задовольняють потреби організації.

Крім того, дослідження моделі даних може підтримувати аналітику даних та виявлення нових залежностей. Воно дозволяє виявити тенденції, зробити прогнози та здійснити стратегічне планування на основі наявних даних. Це дає організації конкурентну перевагу та можливість приймати обґрунтовані рішення.

У загальному висновку, дослідження Nessus, SIEM, Splunk та моделі даних є важливими етапами для забезпечення безпеки, аналізу та ефективного управління даними в організаціях. Вони допомагають виявляти вразливості, моніторити події, аналізувати дані та створювати моделі, що відповідають потребам організації.

РОЗДІЛ 3. ПОБУДОВА ДАТА МОДЕЛІ ТА ВІЗУАЛІЗАЦІЯ ДАНИХ

3.1 Технічні відомості:

- Я буду виконувати роботу на операційній системі Ubuntu 20.04 LTS, так як вона в мене вже була встановлена на моїй машині і добре підходить для виконання цієї роботи.
- В якості SIEM я буду використовувати Splunk, так як це вже відома мені система, до того ж вона є перевіреною, добре вивченою системою і по ній є достатньо багато технічної документації
- Дані про вразливості я буду отримувати зі сканера вразливостей Nessus Expert, так як він теж є добре вивчений і добре інтегрується зі Splunk за допомогою різних Add-on'ів

3.2 Встановлення та отримання даних зі сканера вразливостей Nessus та їх інтеграція в SIEM Splunk. Показувати увесь процес встановлення сканера та SIEM Splunk та їх налаштування сенсу немає, адже це не є основною метою роботи.

3.3 Отримання даних. Після встановлення сканера нам потрібно отримати дані про вразливості, для цього я налаштував та запустив сканування по своїй локальній мережі, вона може виступати лише симуляцією реальних умов в організації та і мало ймовірно, що будь-яка організація надала б мені можливість дізнатись, які вразливості у них присутні, і поширити ці дані, адже це б потягнуло за собою великі ризики. Знизу приведу схему моєї мережі (Рисунок 3.1)



Рисунок 3.1

3.4 Інтеграція даних. Після налаштування і проведення сканування потрібно зробити так, щоб дані автоматизовано інтегрувались в Splunk для їх подальшого опрацювання. Сканування буде проводитись автоматично через певний інтервал часу. Для інтеграції використаємо Nessus API, генеруємо пару ключів для доступу, результат можна побачити на рисунку 3.2

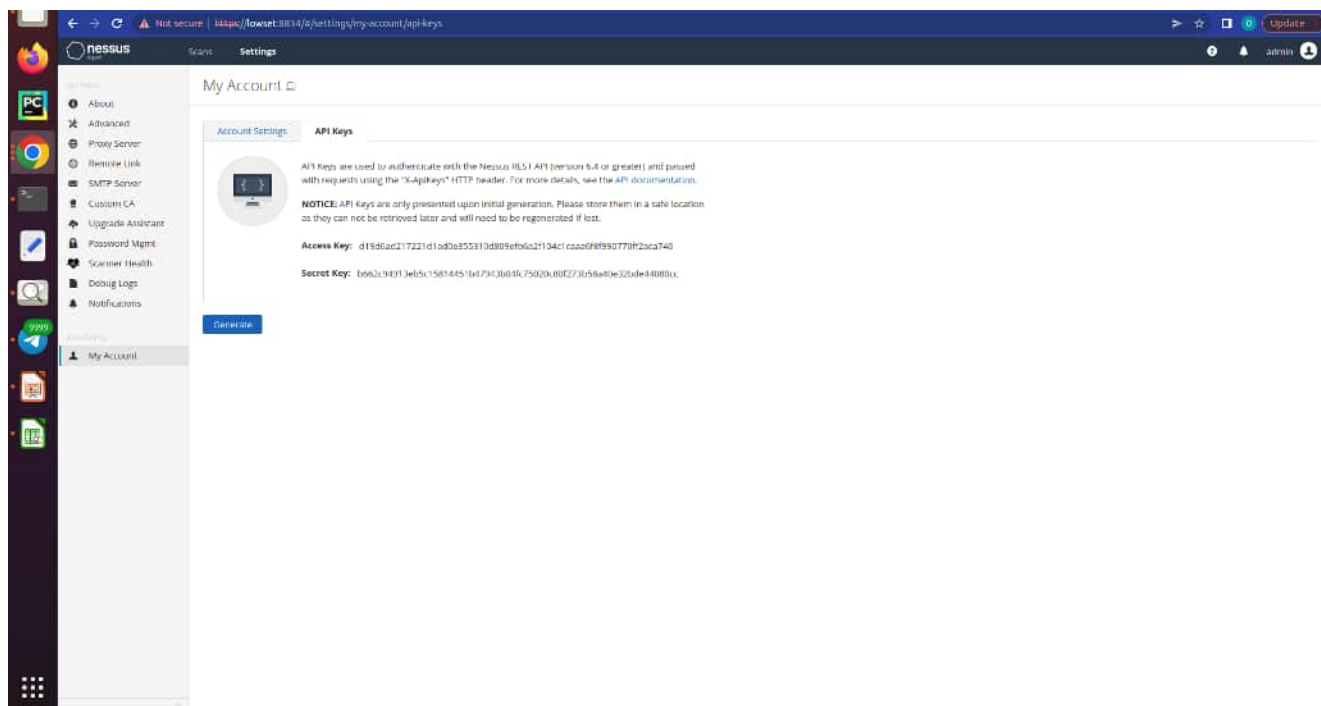


Рисунок 3.2

3.5 Передача даних. В якості допоміжної ланки використаємо Add-on Nessus Add-on Data та скрипт, написаний на мові програмування Python. Для коректної роботи скрипта потрібно вказати наші ключі, які ми згенерували для Nessus API і IP-адресу сервера, на якому в нас працює Nessus, результат можна побачити на рисунку 3.3

```
#!/usr/bin/env python
import requests, json, sys, os, time,datetime

'''
uncomment the line below in order to disable ssl warnings
'''
requests.packages.urllib3.disable_warnings()

'''
URL of Nessus scanner
'''
url = 'https://127.0.0.1:8834'

'''
Uncomment and enter your username and password. Starting with Nessus version 6.4+, api keys are preferred, you may enter the keys instead of username and password.
'''
username = 'gandalf!'
password = 'thehobbit!'

'''
If you want to import specific scans , you will specify them under this comment.
example : scan id's 4,078,34 would look like this sa = [4,078,34]
'''
#sa = [4,078,34]
#sa = []

'''
you can customize drop and pickup directories below
defaults defined
'''
dropdir = '/opt/splunk/etc/apps/TA-nessus_json/drop'
pickupdir = '/opt/splunk/etc/apps/TA-nessus_json/pickup'

verify = False
token = ''

sid = ''
hid = ''
fid = ''
file_id = ''
pid = ''
botd = ''
count = 0

'''
Enter your nessus api access keys here , version 6.4+ allows you to create api keys. Please refer to nessus documentation for nessus 6.4+
'''
accesskey = 'c1888e6c2bcac03a7b0491b272fc7b4bc1d73e33524338f41349b59e0eb1'
secretkey = 'f83eabedf07b08b0e315fba38c4d2d3b4f98bb2f8e2222a4c774af87e1d'

def login(usr, pwd):
```

Рисунок 3.3

Після введення даних в скрипт його потрібно запустити за допомогою команди `python3 <Шлях до директорії, де в нас знаходиться файл зі скриптом>`

3.6 Тегування даних. Тепер дані автоматично завантажуються в SIEM Splunk, і ми можемо до них доступитись за допомогою пошукового запиту по індексу, проте наша ціль – це можливість доступитись до даних через дата мотель. Для цього створимо власне поле `m_tag` для того, щоб наша дата модель могла ідентифікувати дані не лише по індексу, це додає гнучкості в їх відборі. Процес можна побачити на рисунку 3.4

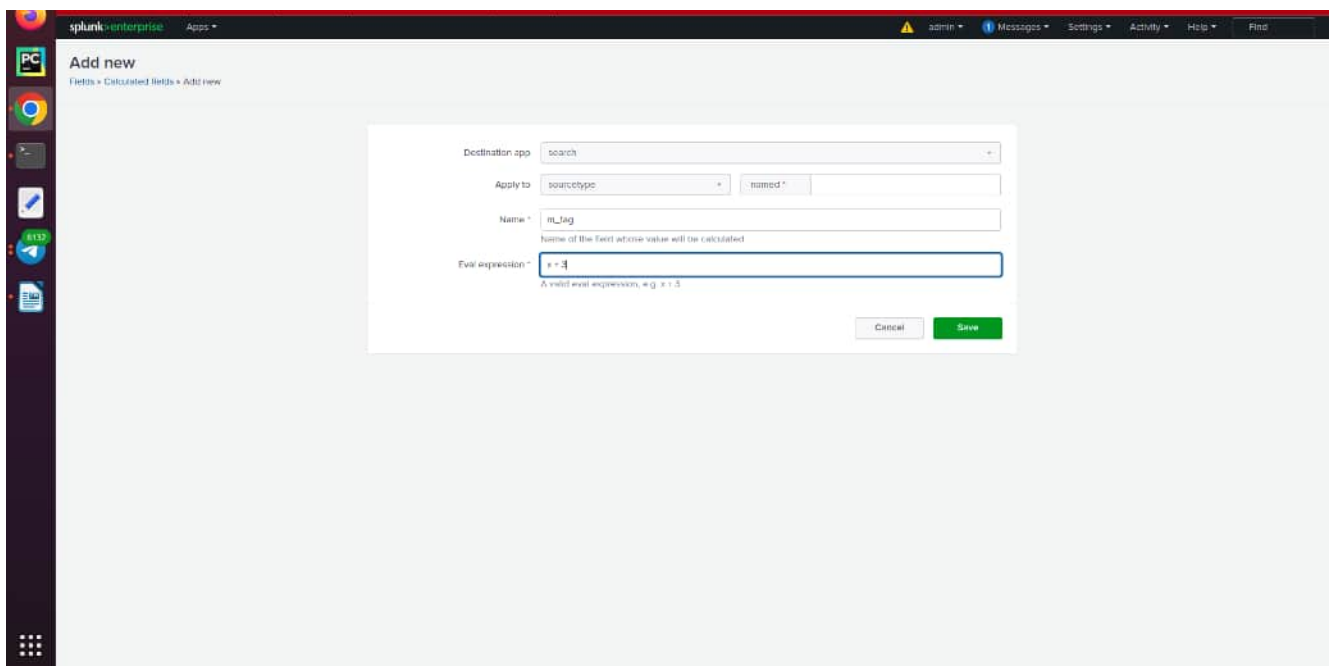


Рисунок 3.4

3.7 Додавання нового поля до даних. Після створення нового поля його потрібно додати до наших даних, які ми отримали зі сканера вразливостей. Процес додавання і команду, яку я використав, можна побачити на рисунку 3.5

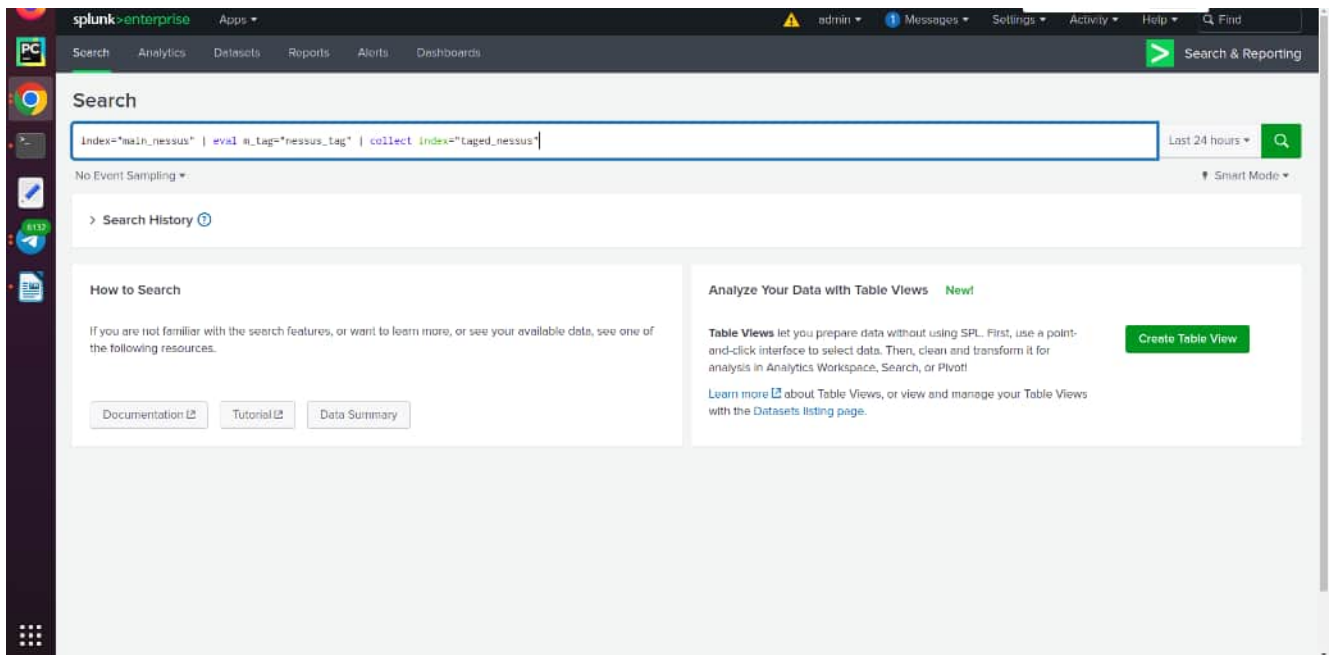


Рисунок 3.5

3.8 Додавання індексу до дата моделі. Для того, щоб дані з індекса підтягувались в нашу датамоделю використовуємо Add-on Splunk Common Information Model, заходимо в налаштування і вибираємо нашу дата модель Vulnerabilities, її додатково встановлювати не потрібно, так як вона є встановлена в Splunk Enterprise по замовчуванню. Знайшовши потрібну дата модель в списку наявних, вписуємо індекс, з якого ми хочемо отримувати дані в нашу датамоделю в поле Indexes whitelist. Це дуже зручно якщо у вас може бути декілька індексів, таке може трапитись, якщо ви використовуєте декілька сканерів вразливостей, їх всіх можна перерахувати в цьому полі, і всі дані з них будуть підтягуватись в дата модель. Детальніше процес можна побачити на рисунку 3.6.

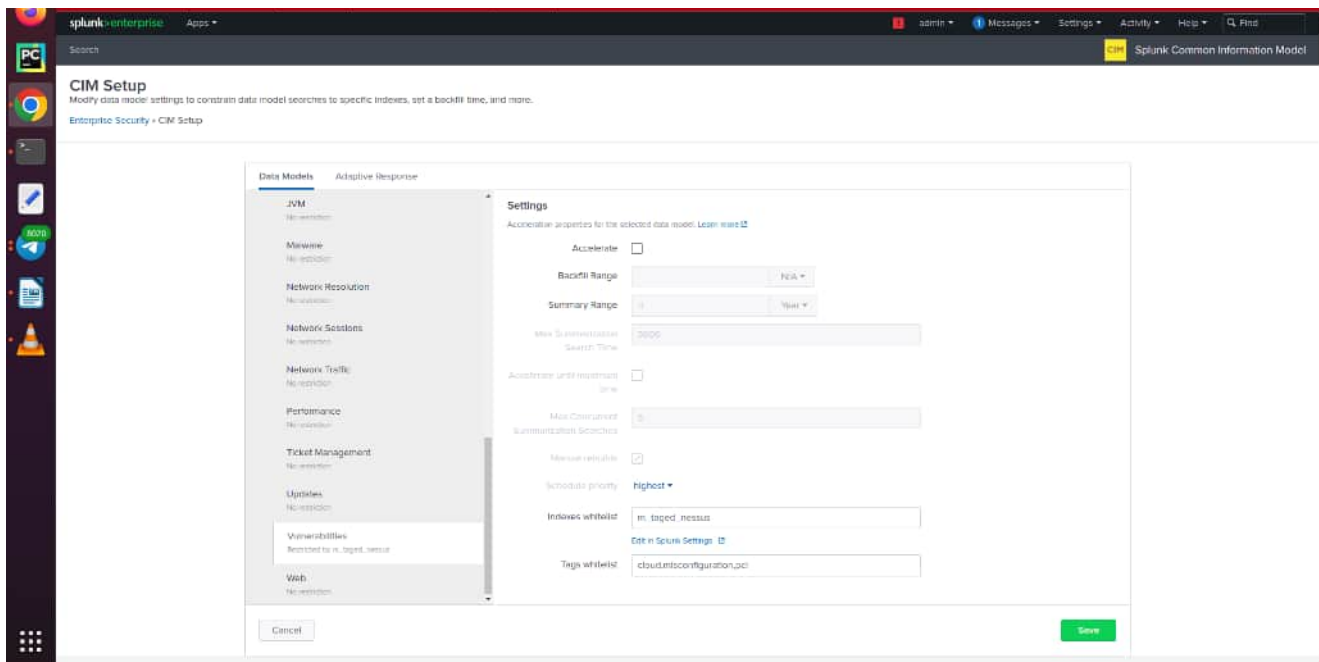


Рисунок 3.6

3.9 Відсіювання даних з індексу за допомогою нового поля `m_tag`.

Після додавання даних в дата модель по індексу нам потрібно відсортувати дані, які призначені лише для дата моделі `Vulnerabilities`, для цього використовуємо поле `m_tag`, яке створили раніше. В налаштуваннях дата моделі є можливість накласти обмеження на дані, а саме в `CONSTRAINTS` вписуємо, що наші дані повинні підтягуватись зі списку індексів і тільки по певних критеріях, в нашому випадку це `тег`. Все це можна побачити на рисунку 3.7.

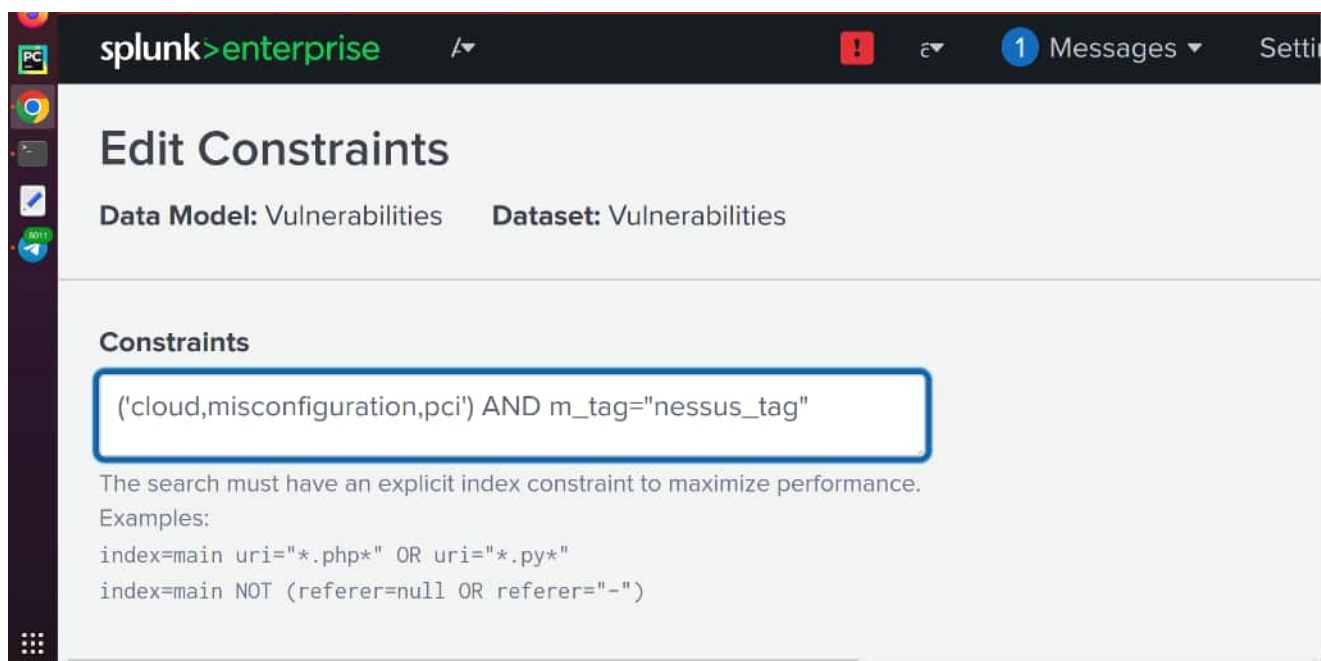


Рисунок 3.7

3.10 Адаптація даних зі сканера до дата моделі.

Дата модель Vulnerabilities по замовчуванню має набір полів, які безпосередньо пов'язані з вразливостями і їх менеджментом, але ці поля в дата моделі і в даних, які приходять зі сканера вразливостей, можуть відрізнитись назвою, при цьому можуть мати одне і те ж значення. Можна додати ці поля вручну в дата модель, але що ж робити, якщо потрібно працювати з декількома сканерами, адже в них для цих полів можуть бути ще інші назви або ж банально може відрізнитись верхній і нижній регістр символів, дублювання полів тут не допоможе, адже ці дані не можна буде опрацьовувати як одне поле. Для вирішення цієї проблеми я використаю Aliases. Псевдоніми допомагають нормалізувати всі дані під певні стандарти, вони працюють таким чином, що коли ми їх створюємо, то вказуємо ім'я поля, для якого потрібно створити псевдонім і сам псевдонім. В процесі створення дані, які записані в поле, для якого ми створюємо псевдонім, продублюються, але вже з іншим іменем, яке підходить дата моделі. На рисунках 3.8 та 3.9 показано, які псевдоніми я створював.

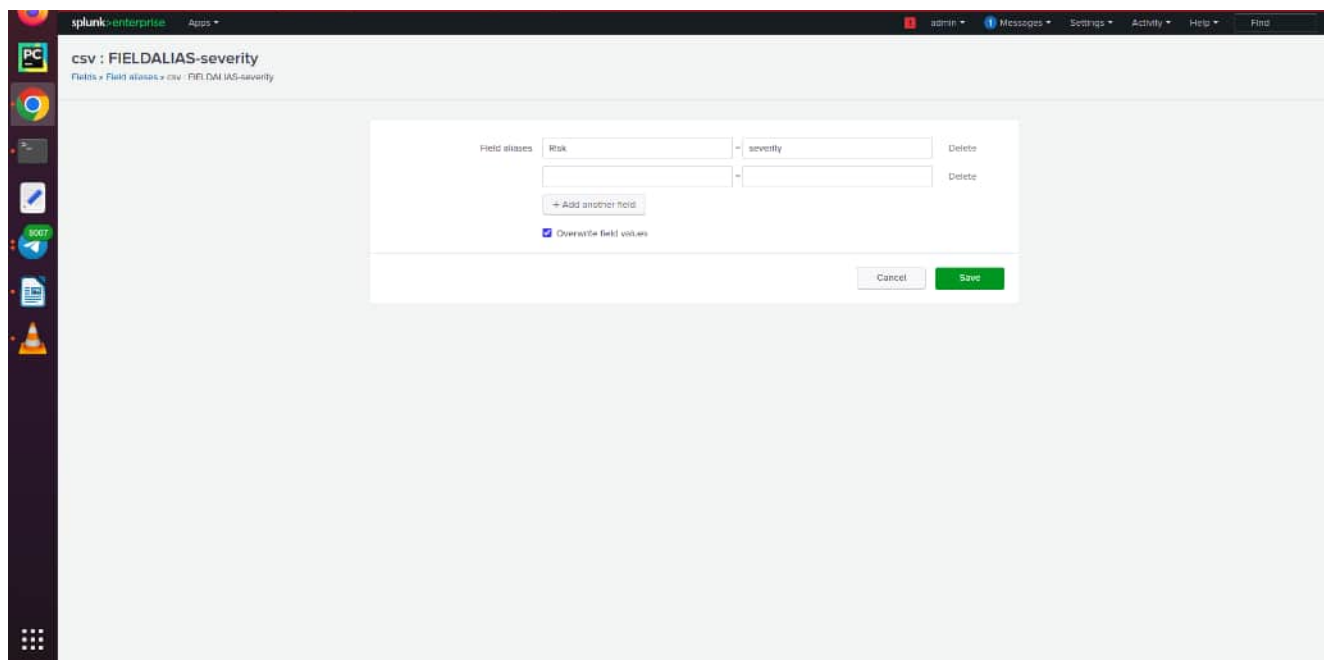


Рисунок 3.8

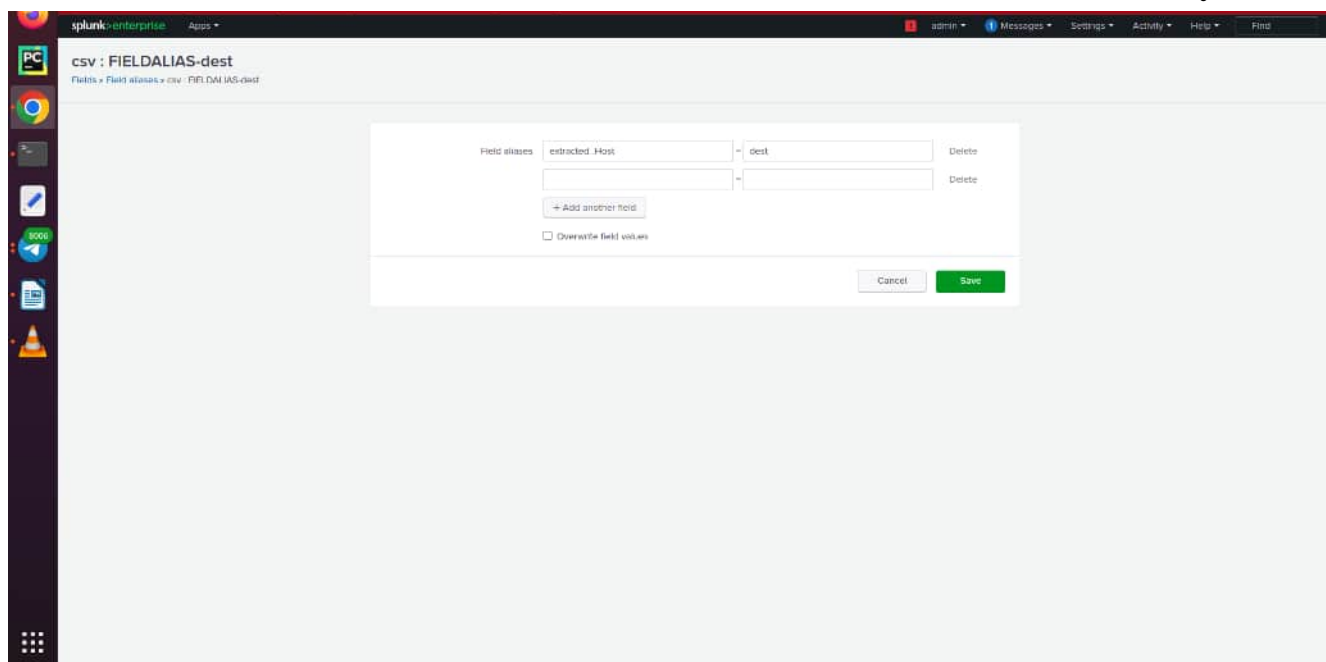


Рисунок 3.9

3.11 Додавання полів в дата модель. Може бути таке, що в дата моделі немає полів, які вам потрібні, ми можемо їх додати в датамодель, вибравши дані, які ми вже отримуємо. Вікно, в якому ми це можемо зробити, можна побачити на рисунку 3.10.

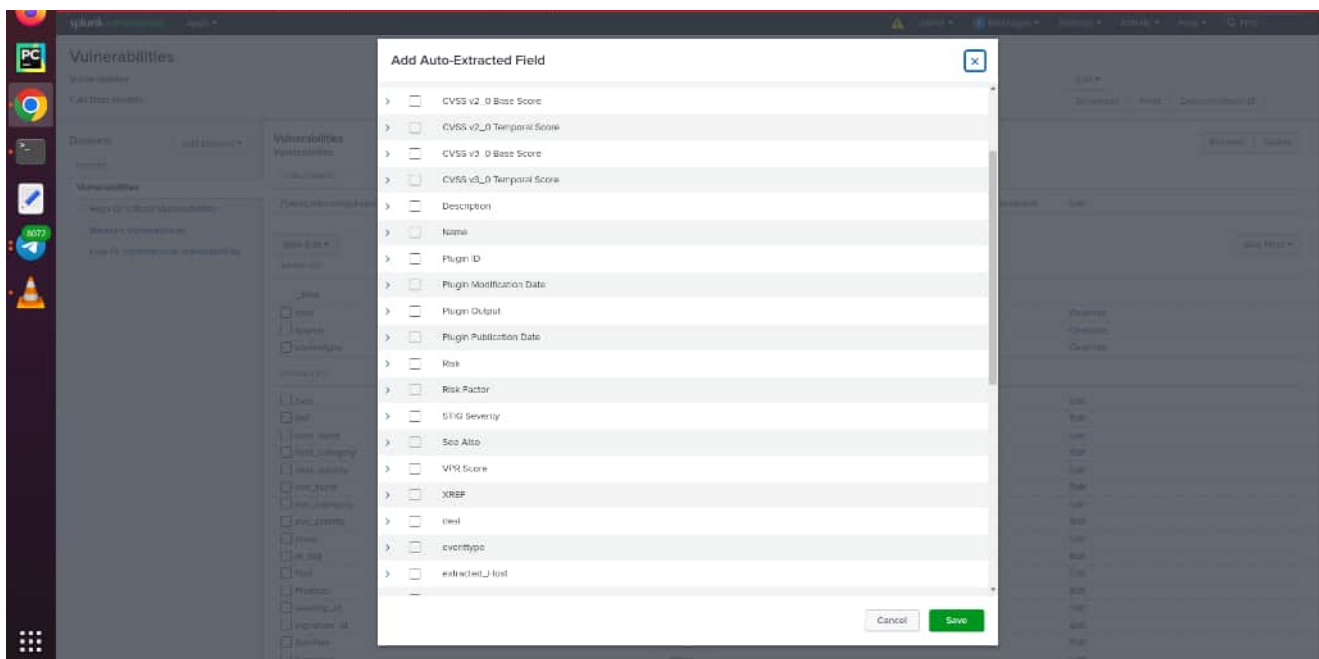


Рисунок 3.10

3.12 Отримання даних з дата моделі. Після всіх виконаних процедур ми можемо побудувати дашборд на основі даних з дата моделі. Приклад запиту на отримання даних і їх візуалізацію можемо бачити на рисунку 3.11

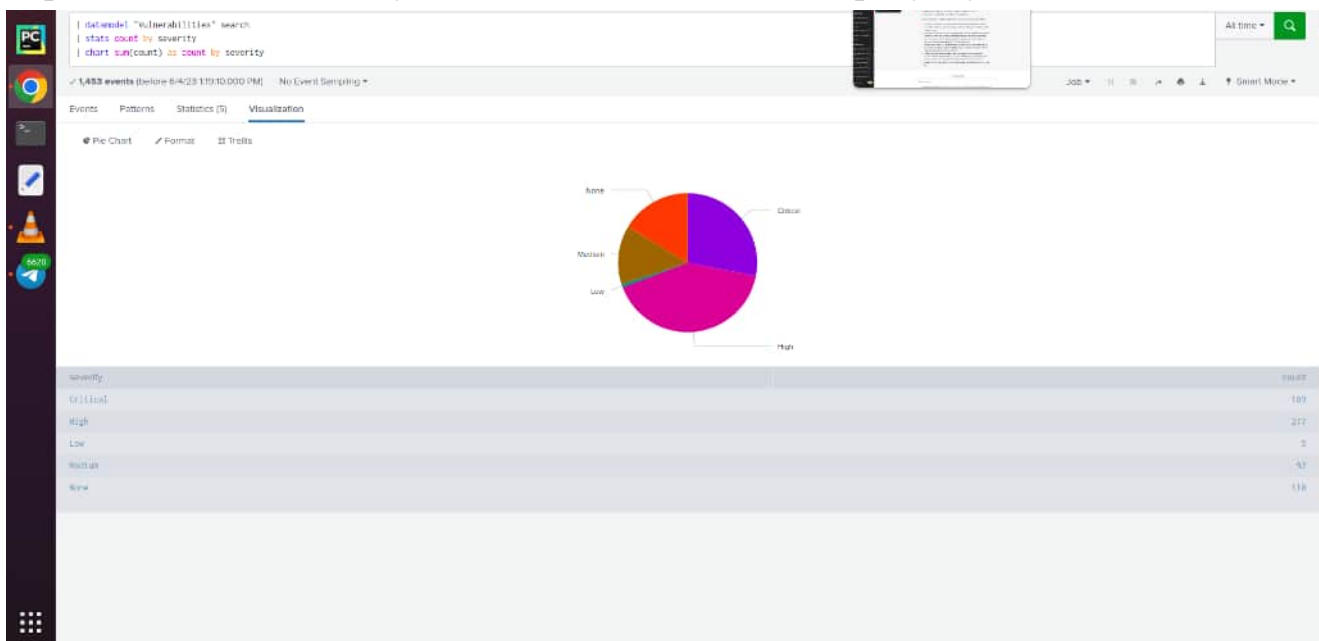


Рисунок 3.11

3.13 Візуалізація даних. Описувати те, як я візуалізував дані, сенсу немає, адже це не є ціллю цієї роботи. Результати візуалізації можна побачити на рисунках 3.12, 3.13, 3.14

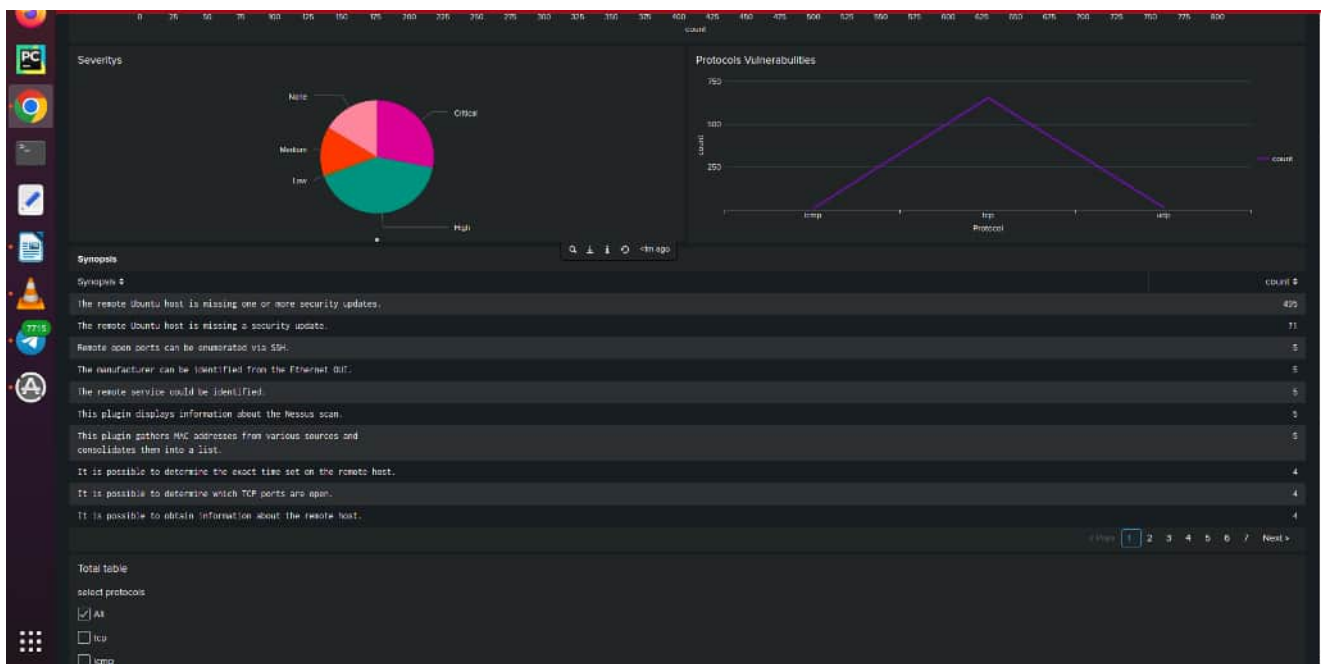


Рисунок 3.12

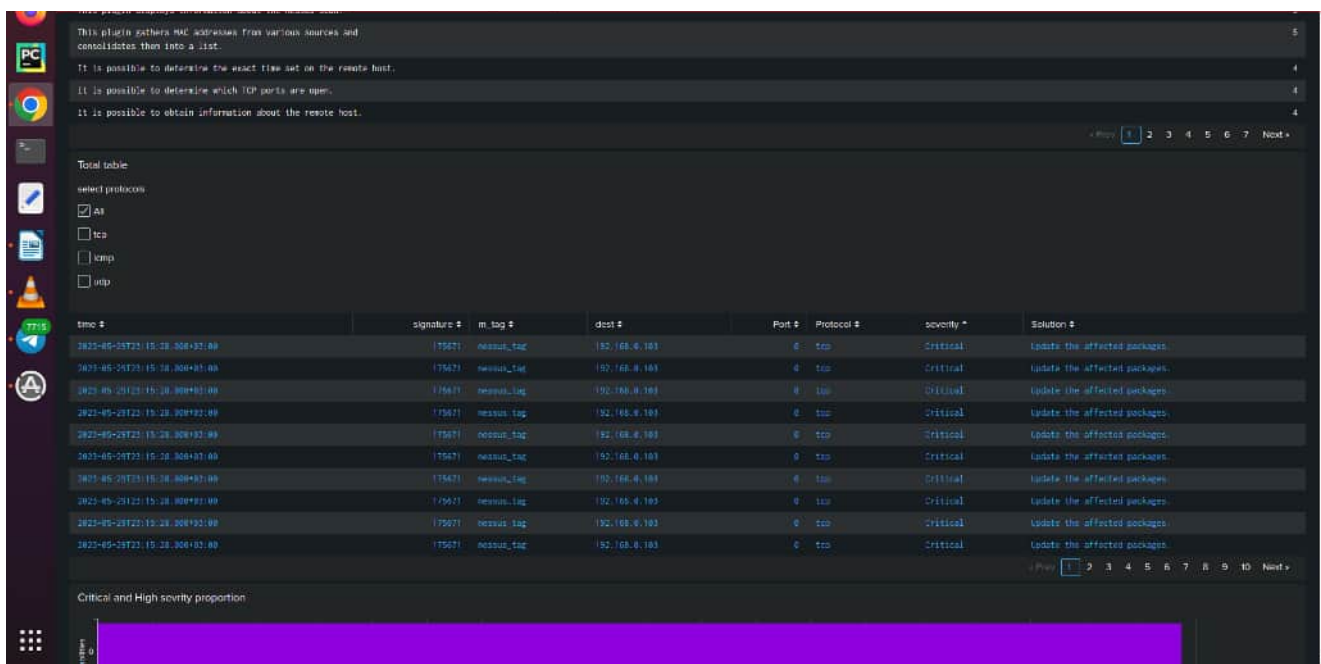


Рисунок 3.13

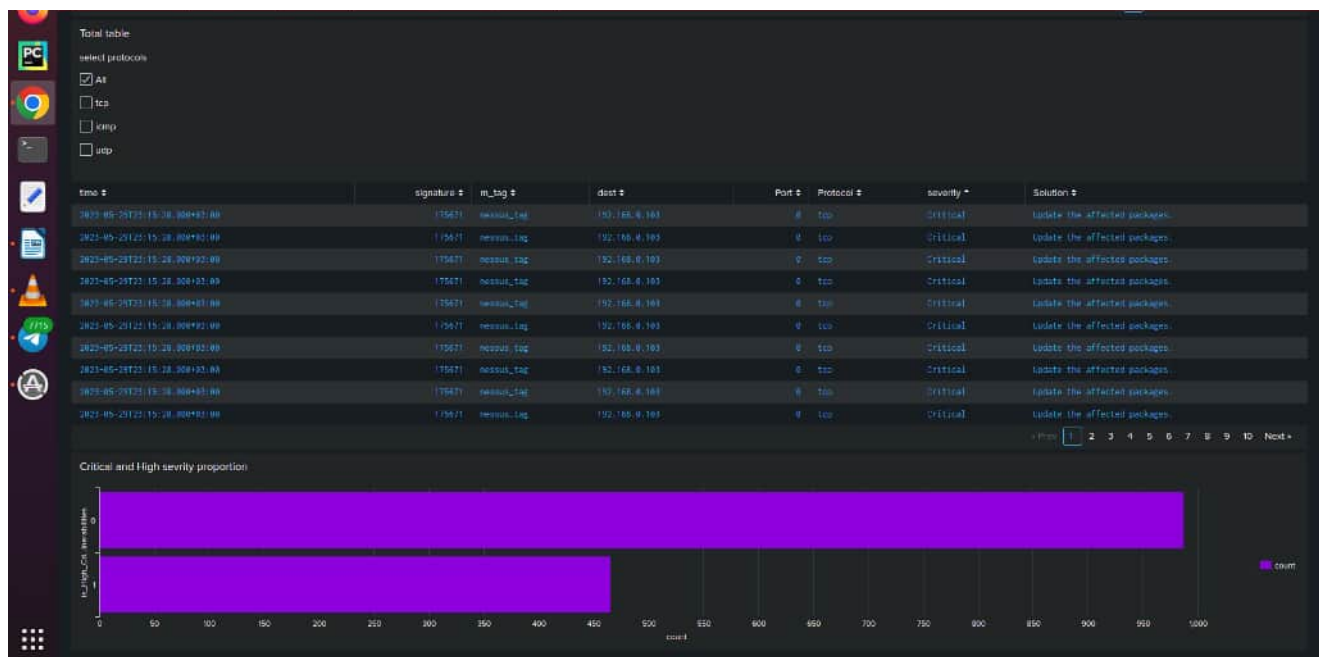


Рисунок 3.14

Висновки до розділу 3.

В цьому розділі було показано процес автоматизації передачі даних зі сканера вразливостей Nessus в SIEM Splunk. Для цього були вивчені і використанні різноманітні системи та інструменти як в самому сканері (такі як Nessus API), так і в SIEM (такі як різні Add-on'и). Також використовувались і сторонні інструменти, наприклад мова програмування Python. Ця робота полягала у інтеграції можливостей одного інструмента в інші, використовуючи можливості самих інструментів та сторонніх. В результаті ми отримали можливості бачити опрацьовані і візуалізовані дані, до того ж вони автоматично оновлюються, що дає можливість спостерігати ситуацію в реальному часі.

ВИСНОВКИ

У даній дипломній роботі була розглянута тема побудови менеджменту вразливостей з використанням сканера вразливостей Nessus та інструменту аналізу даних Splunk. Робота ставила за мету встановити сканер вразливостей Nessus, налаштувати його та автоматизувати передачу зібраних даних в Splunk. На основі отриманих даних було побудовано дашборд, що надає зручну інформацію для аналізу та керування вразливостями в інформаційній системі.

Результати дослідження показали, що використання сканера вразливостей Nessus у поєднанні з інструментом аналізу даних Splunk є ефективним підходом до побудови менеджменту вразливостей. Завдяки автоматизованій передачі даних зі сканера вразливостей до Splunk забезпечується швидкий та зручний доступ до актуальної інформації про вразливості системи.

Дашборд, побудований на основі зібраних даних, надає зрозумілу та зручну візуалізацію інформації, що допомагає адміністраторам та керівникам приймати обґрунтовані рішення з пріоритетизації вразливостей та планування заходів щодо їх вирішення. Дашборд також дозволяє відслідковувати ефективність заходів, вжитих для ліквідації вразливостей.

Застосування побудови менеджменту вразливостей з використанням Nessus та Splunk допомагає забезпечити безпеку інформаційної системи, знижує ризики вразливостей та підвищує рівень захищеності. Отримані результати можуть бути використані в організаціях для покращення процесу управління вразливостями та забезпечення надійності та безпеки інформаційних ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. SIEM: [[Веб-сайт](#)].
2. Splunk Documentation: [[Веб-сайт](#)]
3. Nessus Documentation: [[Веб-сайт](#)]
4. Комп'ютерна безпека: [[Веб-сайт](#)]
5. SPL Documentation: [[Веб-сайт](#)]
6. Splunk tutorial: [[Веб-сайт](#)]
7. Data Model Documentation: [[Веб-сайт](#)]