ЛАБОРАТОРНА РОБОТА №2

ДОСЛІДЖЕННЯ SIEM-СИСТЕМИ WAZUH

Мета роботи:

1. Ознайомлення з призначенням та архітектурою SIEM-системи Wazuh.
2. Дослідження можливостей збору, обробки та аналізу подій інформаційної безпеки в системі Wazuh.

Інструменти та ПЗ: Kali Linux, SIEM-система Wazuh.

Теоретичні відомості

SIEM (Security Information and Event Management) – це система управління інформацією та подіми безпеки. Вона виконує наступні функції:

1. Збір логів з різних джерел (сервери, мережеві пристрої, додатки).
2. Аналіз та кореляція подій безпеки в режимі реального часу.
3. Виявлення загроз на основі ппередньо налаштованих правил.
4. Генерацію сповіщень про потенційні інциденти безпеки.
5. Зберігання логів для форензичного аналізу та відповідності нормативним вимогам.

Архітектура Wazuh

Wazuh складається з трьох основних компоненів:

1. Wazuh Manager (Менеджер).
2. Wazuh Indexer (Індексатор).
3. Wazuh Dashboard (Дашборд).

Wazuh Manager є центральним компонентом системи, який отримує та обробляє дані від агентів. Він виконує кореляцію подій безпеки та застосовує правила виявлення загроз, а також зберігає конфігураційні дані і здійснює керування агентами.

Wazuh Indexer базується на платформі OpenSearch та призначений для індексації й зберігання даних інформаційної безпеки з метою забезпечення швидкого та ефективного пошуку. Крім того, даний компонент забезпечує масштабованість SIEM-системи.

Wazuh Dashboard являє собою веб-інтерфейс для візуалізації зібраних даних. Він надає інструменти для аналізу подій безпеки, формування звітів, а також використовується для конфігурації та централізованого управління системою.

Агенти Wazuh

Агенти Wazuh – це програмні компоненти, які встановлюються на моніторингових системах з метою збору журналів файлів і системних подій. Вони здійснюють моніторинг цілісності файлів, забезпечують виявлення аномалій та підозрілої активності, а також передають зібрані дані до центрального компонента системи – Wazuh Manager.

Правила та декодери

Правила (Rules) – це логічні конструкції, які визначають, які події слід вважати підозрілими або зловмисними. Вони також встановлюють рівень притичності загроз у діапазоні від 0 до 15, а також визначають категорії загроз і групи правил для подальшої класифікації подій безпеки.

Декодери (Decoders) – є компонентами системи, які виконують розбір вхідних журналів подій та виділяють їх структурні елементи. Вони забезпечують підготовку даних для подальшого застосування правил, а також здійснюють нормалізацію форматів даних, отриманих з різних джерел.

Інтеграція з MITRE ATT&CK

SIEM-система Wazuh інтегрується з фреймворком MITRE ATT&CK з метою картування виявлених загроз відповідно до тактик і технік зловмисників. Така інтеграція дозволяє краще розуміти повний ланцюжок кібератаки, а також сприяє підвищенню ефективності та вдосконаленню стратегій захисту інформаційних систем.

Завдання на лабораторну роботу

Завдання 1. Розгортання та доступ до Wazuh.

1. Запустіть групу сервісів Wazuh:

   sudo ./lab-management.sh start wazuh

```
NAME              IMAGE                              COMMAND                  SERVICE
EATED        STATUS          PORTS
wazuh-dashboard   wazuh/wazuh-dashboard:4.13.0   "/entrypoint.sh"         wazuh.dashboard
 days ago   Up 4 minutes   443/tcp, 0.0.0.0:443→5601/tcp, [::]:443→5601/tcp
wazuh-indexer     wazuh/wazuh-indexer:4.13.0     "/entrypoint.sh open…"   wazuh.indexer
 days ago   Up 4 minutes   9200/tcp
wazuh-manager     wazuh/wazuh-manager:4.13.0     "/init"                  wazuh.manager
 days ago   Up 4 minutes   1514-1516/tcp, 514/udp, 55000/tcp
```

Рисунок 1 – Успішний запуск групи сервісів Wazuh

2. Відкрийте браузер та перейдіть за адресою:

   https://localhost:443

3. Увійдіть до системи з обліковими даними:

   Username: *admin*

   Password: *SecretPassword*

4. Переконайтеся, що головна сторінка дашборду завантажилася успішно.

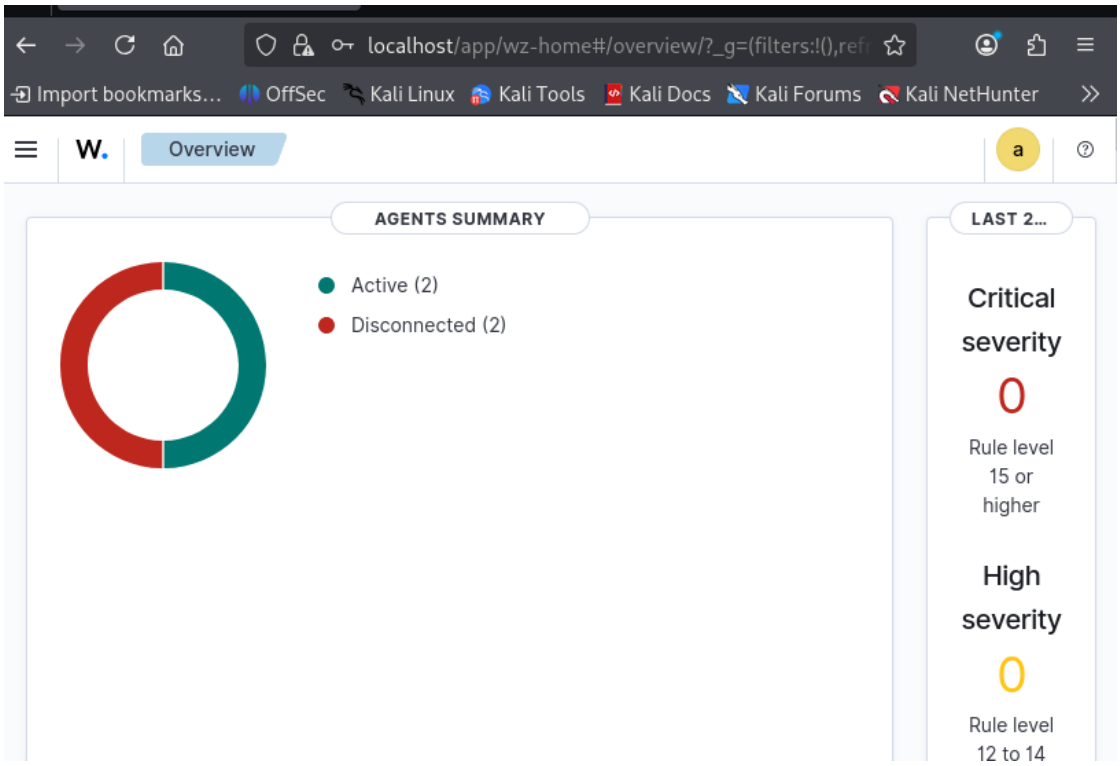

Рисунок 2 – Головна сторінка Wazuh Dashboard

Завдання 2. Дослідження основного інтерфейсу.

1. На головній сторінці ("Overview") зверніть увагу на наступну інформацію:

- Загальна кількість агентів (до розгортання навчальних веб-сайтів агенти можуть бути відсутні).

- Загальна кількість сповіщень за останню добу.

2. Розгорність секції у лівому меню та ознайомтеся з модулями:

- Explore → Discover – моніторинг подій безпеки.

- Endpoint security → File Integrity Monitoring – контроль цілісності файлів.

- Threat intelligence → Vulnerability Detection – виявлення уразливостей.

- Endpoint security → Configuration Assessment – оцінка конфігурації безпеки.

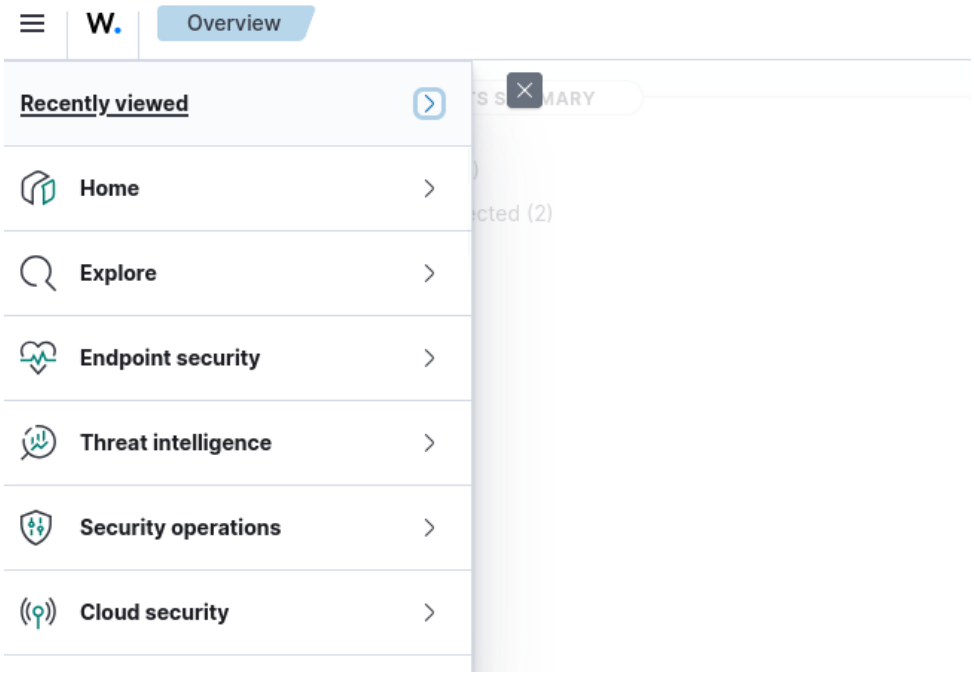

Рисунок 3 – Перелік секцій

3. Перейдіть до модуля “Discover” та ознайомтеся з інтерфейсом:

- Часова шкала подій.

- Таблиця деталізованих подій.

- Панель фільтрів.

4. Розгорніть секцію “Server management” і “Agents management” та ознайомтеся з компонентами:

   - Rules – управління правилами виявлення.

   - Decoders – управління декодерами.

   - Groups – управління групами агентів.

   - Summary – упрвління агентами.

Завдання 3. Аналіз структури правил.

1. Перейдіть до “Server management” → “Rules”.
2. У пошуку введіть “sshd”.

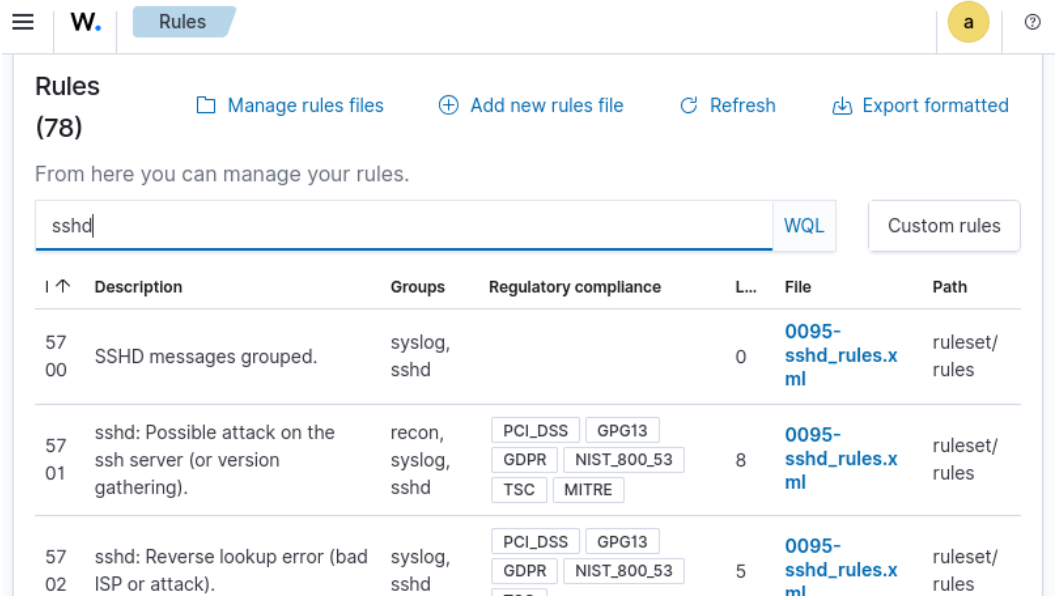

Рисунок 4 – Пошук правил за ключовим словом “sshd”

3. Знайдіть правило з ID 5716 та проаналізуйте його структуру:

```
<rule id="5716" level="5">
  <if_sid>5700</if_sid>
  <match>^Failed|^error: PAM: Authentication</match>
  <description>sshd: authentication failed.</description>
  <mitre>
    <id>T1110</id>
  </mitre>
  <group>authentication_failed,gdpr_IV_35.7.d,gdpr_IV_32.2,
gpg13_7.1,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,pci_dss_10.2.
4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
 </rule>
```

4. Знайдіть наступні значення:

ID правила, рівень критичності, опис правила, умови спрацьовування.

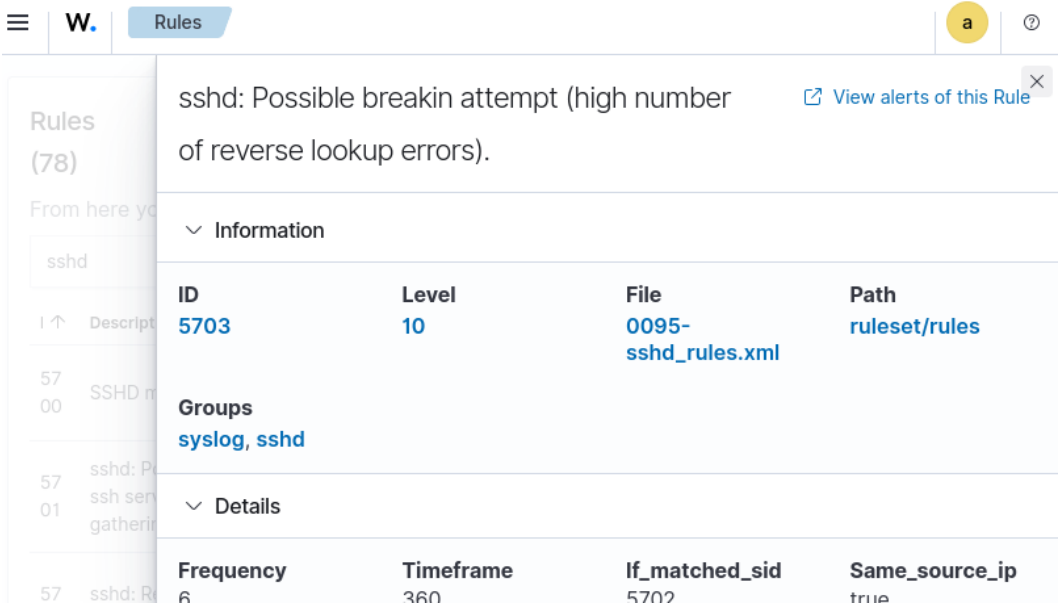

Рисунок 5 – Приклад детальної інформації про правило Wazuh

5. За допомогою пошуку знайдіть та проаналізуйте по одному правилу з наступних категорій:

- Web attacks (файл веб-атак).
- Windows (файл Windows подій).
- Firewall (файл мережевих подій).

6. Перейдіть до "Server management" → "Decoders". Оберіть декодер "sshd", дослідіть його структуру та принцип підготовки даних для правил.

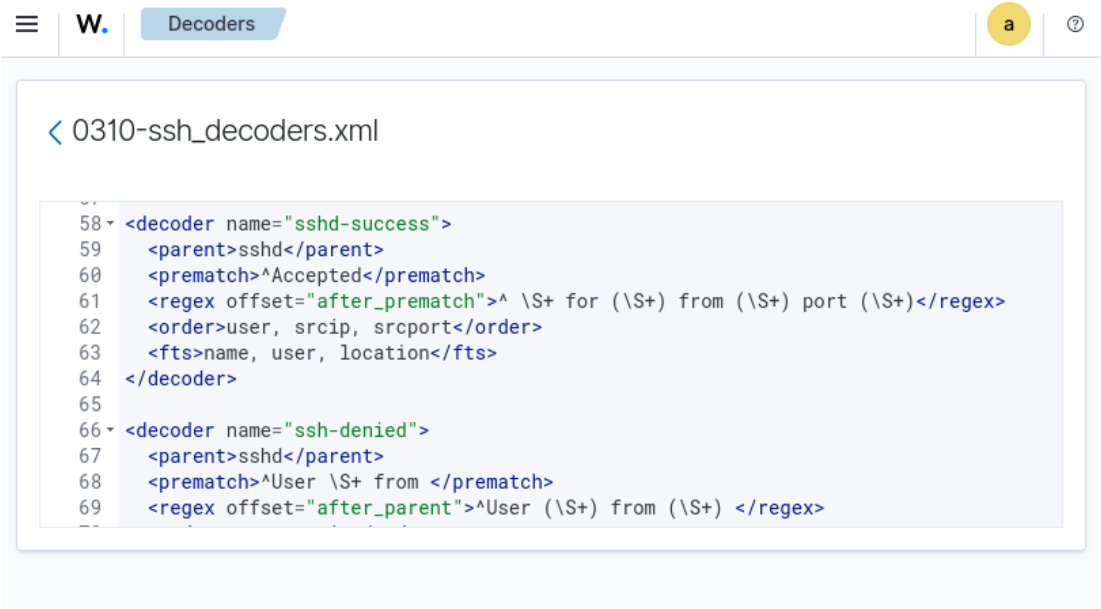

Рисунок 6 – Приклад структури SSH-декодера

Завдання 4. Управління агентами та конфігурацією.

1. Перейдіть до "Agents management" → "Summary".

2. Дослідіть інтерфейс управління агентами:

- Список агентів.

- Статуси агентів.

- Кнопка “Deploy new agent”.

3. Натисність “Deploy new agent” та ознайомтеся з процесом реєстрації агентів для різних операційних систем.

Завдання 5. Дослідження MITRE ATT&CK.

1. Перейдіть до "Threat Intelligence" → "MITRE ATT&CK" та ознайомтеся з тактиками фреймворку (вкладка Framework):

- Initial Access.

- Execution.

- Persistence.

- Defense Evasion.

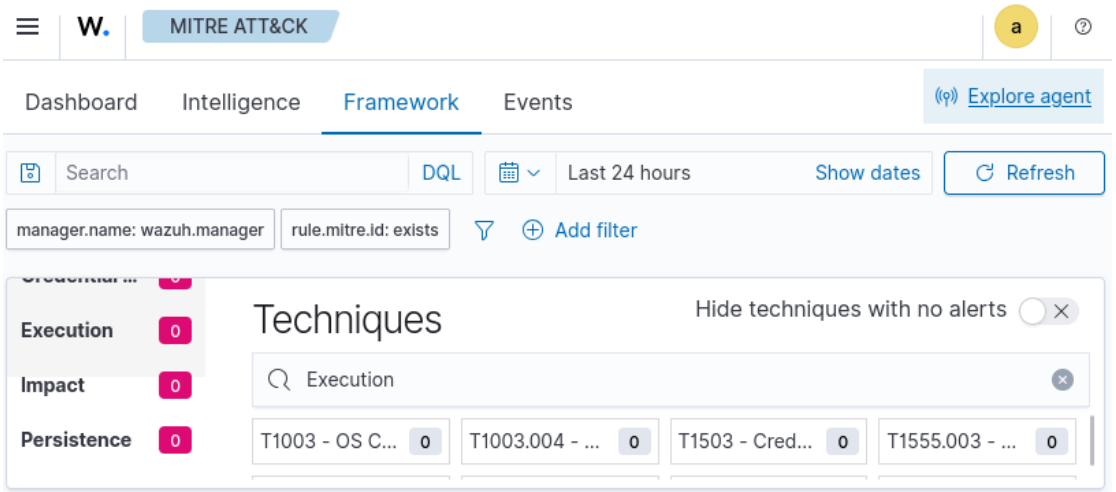

Рисунок 7 – Пошук технік “MITRE ATT&CK” за назвою тактики“Execution”

2. Оберіть одну з тактик та проаналізуйте, які техніки до неї належать.

3. Проаналізуйте детальну інформацію про одну із знайдених технік MITRE ATT&CK.

4. Перейдіть до "Server management" → "Dev Tools".

5. Ознайомтеся з можливостями REST API Wazuh.

6. Спробуйте виконати простий запит для отримання інформації про статус менеджера (шляхом виділення запиту та натискання на кнопку “Run”, що з’являється поруч із запитом).

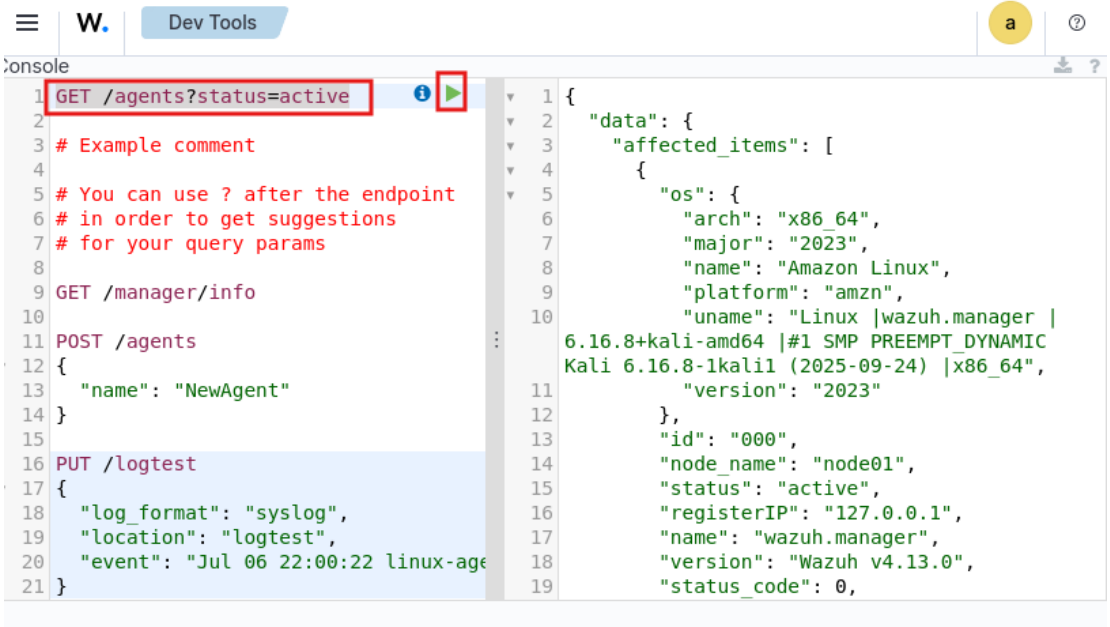

Рисунок 8 – Приклад виконання запиту для отримання інформації про активних агентів

Контрольні запитання

1. Що означає абревіатура SIEM**?**
2. Які основні функції виконує SIEM-система?
3. Які три ключові компоненти входять до архітектури Wazuh?
4. Яке призначення Wazuh Manager?
5. Яке призначення Wazuh Indexer?
6. Яке призначення Wazuh Dashboard?
7. Які основні функції реалізує агент Wazuh на хості?
8. У якому діапазоні визначається рівень критичності подій у правилах Wazuh?