ЛАБОРАТОРНА РОБОТА №3
ДОСЛІДЖЕННЯ АВТОМАТИЗОВАНОГО СКАНУВАННЯ ВРАЗЛИВОСТЕЙ З ВИКОРИСТАННЯМ OPENVAS

Мета роботи:

1. Ознайомлення з принципами автоматичного сканування вразливостей інформаційних систем.

2. Набуття практичних навичок роботи з інструментом OpenVAS.

3. Дослідження процесу виявлення та аналізу вразливостей на вразливій системі Metasploitable2 у середовищі Kali Linux.

Інструменти та ПЗ: VM Kali Linux, OpenVAS, Metasploitable2.

Теоретичні відомості

OpenVAS

OpenVAS (Open Vulnerability Assessment System) – це сканер вразливостей з відкритим вихідним кодом. Він використовується для автоматизованого пошуку вразливостей, відкритих портів, небезпечних сервісів та оцінки безпеки мережевої інфраструктури, генеруючи детальні звіти з рекомендаціями. Після випуску OpenVAS версії 9.0 фреймворк було перейменовано на Greenbone Vulnerability Management (GVM) і випущено як Greenbone Source Edition (GSE). Починаючи з GVM 10, термін OpenVAS використовується тільки для компонента сканера.

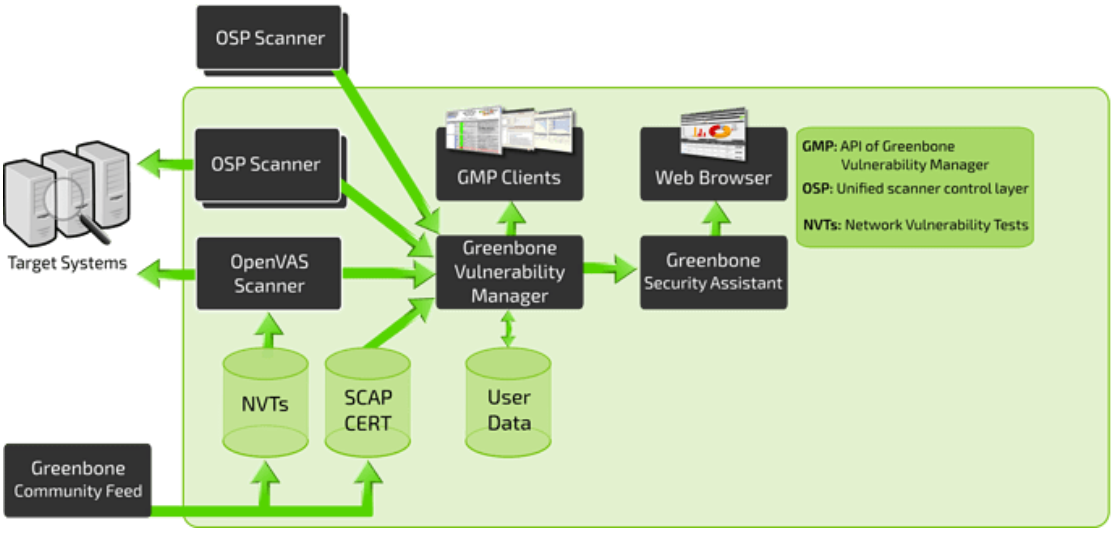

Рисунок 1 – Архітектура фреймворку GVM

Фреймворк GVM має складну архітектуру, яка умовно поділяється на три основні частини:

1. Інтерфейс користувача (Front-End).

2. Серверна частина (Back-End).

3. Система постачання даних про вразливості й інформаційні оновлення.

Клієнтська частина (GSA, вебінтерфейси) являє собою інтерфейс, з яким користувач взаємодіє під час роботи з OpenVAS через веб-браузер. Веб-інтерфейси побудовані на основі Greenbone Security Assistant та спрощують роботу аналітика під час використання OpenVAS та інших сканерів у межах фреймворку GVM.

Серверна інфраструктура (OSP, OpenVAS, цілі сканування) безпосередньо відповідає за виконання сканування вразливостей, обробку даних та тестів NVT за допомогою OpenVAS і компонентів GVM. Greenbone Vulnerability Manager виступає проміжною ланкою між сканерами та користувацькими інтерфейсами фронтенду, забезпечуючи централізоване управління процесом сканування.

Система отримання вразливостей та інформаційних оновлень (NVT, SCAP, CERT, дані користувачів, Community Feed) містить усю інформацію та тести на вразливості, що надходять із Greenbone Community Feed, які використовуються як основна базова платформа для перевірки інформаційних систем. Також передбачена можливість використання користувацьких даних, наданих користувачем, замість стандартних NVT та SCAP/CERT, що постачаються Greenbone.

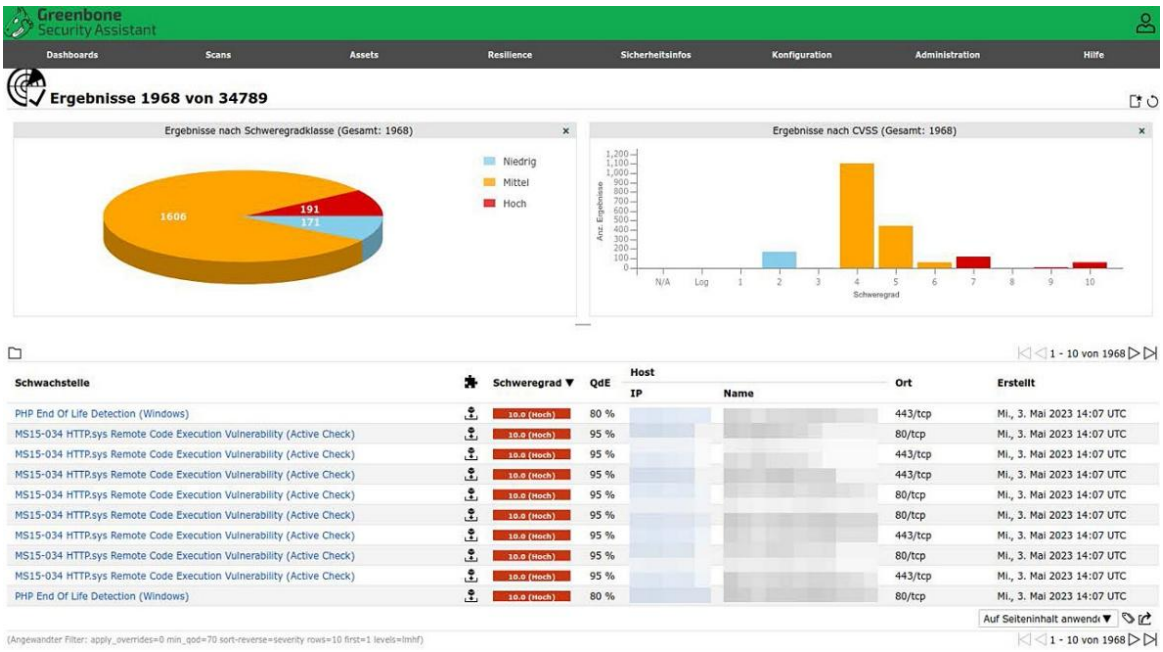

Рисунок 2 – Інтерфейс OpenVAS

NVT

NVT (Network Vulnerability Tests) – це набір спеціалізованих сценаріїв перевірки, які використовуються для виявлення конкретних вразливостей у мережевих сервісах, операційних системах та прикладному програмному забезпеченні. Кожен NVT відповідає певній вразливості або конфігураційній помилці та регулярно оновлюється через Greenbone Community Feed.

CVSS

Для оцінки рівня небезпеки вразливостей використовується стандарт CVSS (Common Vulnerability Scoring System). Оцінка формується за шкалою від 0 до 10 та поділяється на рівні:

1. 0.0 – 3.9 – Low.
2. 4.0 – 6.9 – Medium.
3. 7.0 – 8.9 – High.
4. 9.0 – 10 – Critical.

CVE

CVE (Common Vulnerabilities and Exposures) – це стандартизована система ідентифікації відомих вразливостей інформаційних систем. Вона використовується як фахівцями з атакувального напряму (Red Team), так і

спеціалістами з захисту (Blue Team) для уніфікованого опису та обміну інформацією про вразливості.

Кожній вразливості у межах CVE присвоюється унікальний ідентифікатор. У деяких випадках ідентифікатор може бути опублікований без детального технічного опису, що пов’язано з політикою відповідального розкриття інформації (responsible disclosure).

Ідентифікатор CVE має стандартизований формат:

CVE-YYYY-NNNN, де **YYYY** – рік реєстрації вразливості, а **NNNN** – її порядковий номер.

Рисунок 3 – Приклад CVE-2024-43572 - MMC Remote Code Execution Vulnerability

Завдання на лабораторну роботу

Завдання 1. Імпорт віртуальної машини Kali Linux з курсу Cisco.

1. Завантажити готовий образ віртуальної машини у форматі .ova зі сторінки дисципліни (VM Kali Linux (Cisco)).

2. Запустити середовище Oracle VM VirtualBox.

3. У головному меню обрати пункт “File” → “Import Appliance”

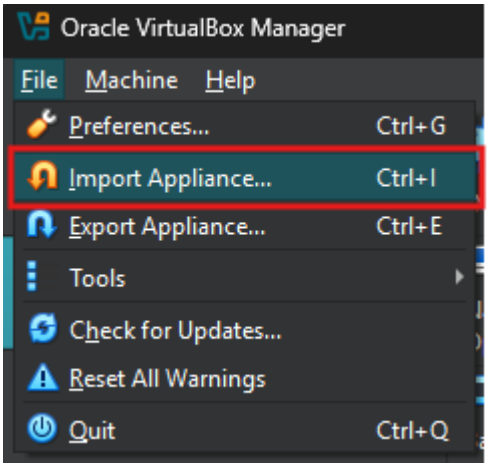

Рисунок 4 – Вкладка “File” → “Import Appliance”

4. У полі “File” обрати завантажений образ віртуальної машини.

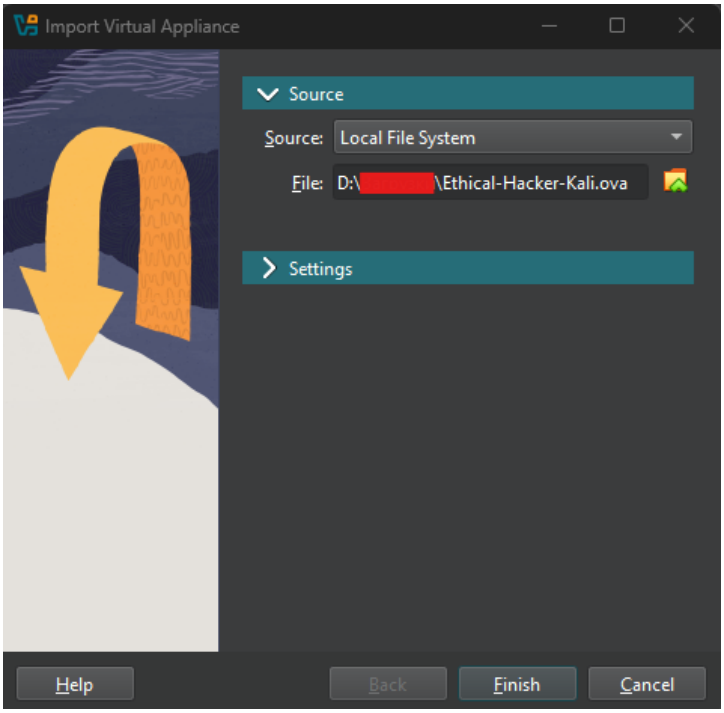

Рисунок 5 – Процес імпорту віртуальної машини Kali Linux у середовище VirtualBox

5. У вікні налаштувань змінити назву віртуальної машини, додавши **власне прізвище**, а також встановити обсяг оперативної пам’яті на рівні 4000 МБ.

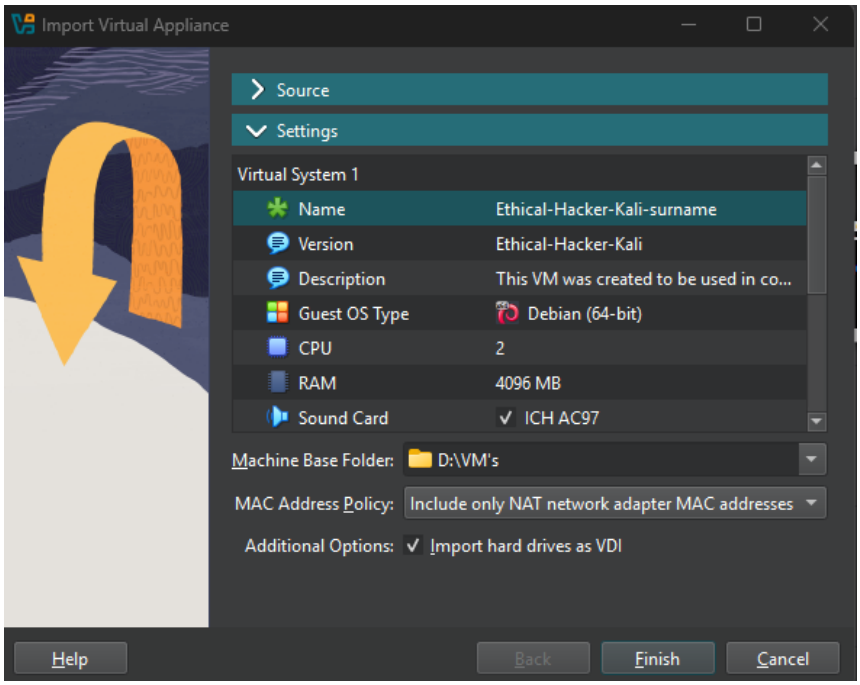

Рисунок 6 – Налаштування параметрів ВМ Kali Linux

6. Натиснути кнопку “Finish” та дочекатися завершення процесу імпорту віртуальної машини до середовища VirtualBox.

Завдання 2. Запуск служби GVM.

1. Запустити віртуальну машину Kali Linux та виконати вхід до системи.

Логін: kali

Пароль: kali

2. Відкрити термінал.

3. Для запуску служби Greenbone Vulnerability Management (GVM) виконати команду:

sudo gvm-start

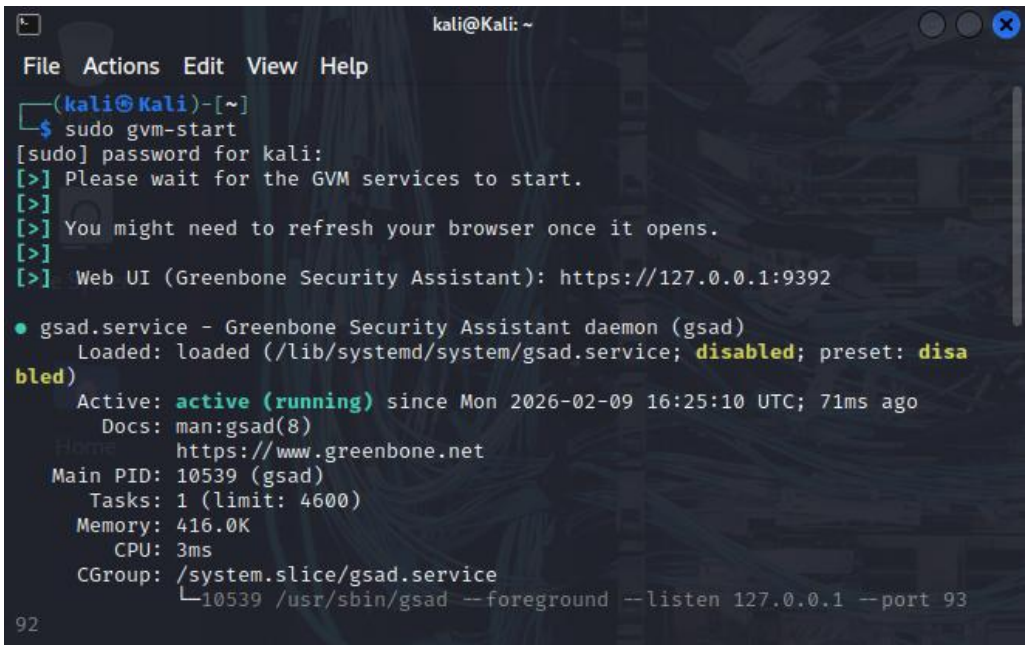

Рисунок 7 – Запуск сервісу GVM (OpenVAS)

4. Дочекатися завершення ініціалізації всіх компонентів GVM.

5. Після успішного запуску служби у веб-браузері відкрити веб-інтерфейс керування, використовуючи адресу:

https://127.0.0.1:9392

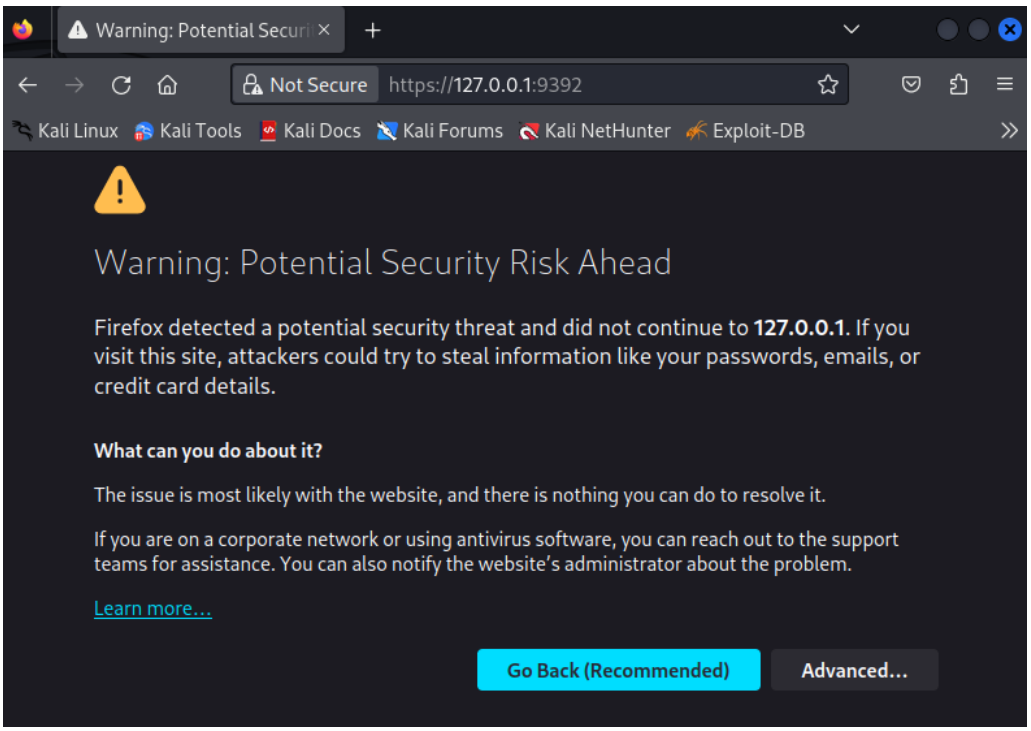

Рисунок 8 – Перехід за адресою ***https://127.0.0.1:9392*** у веб-браузері

6. Переконатися у доступності веб-інтерфейсу GVM та готовності системи до подальшої роботи.

Логін: admin

Пароль: kali

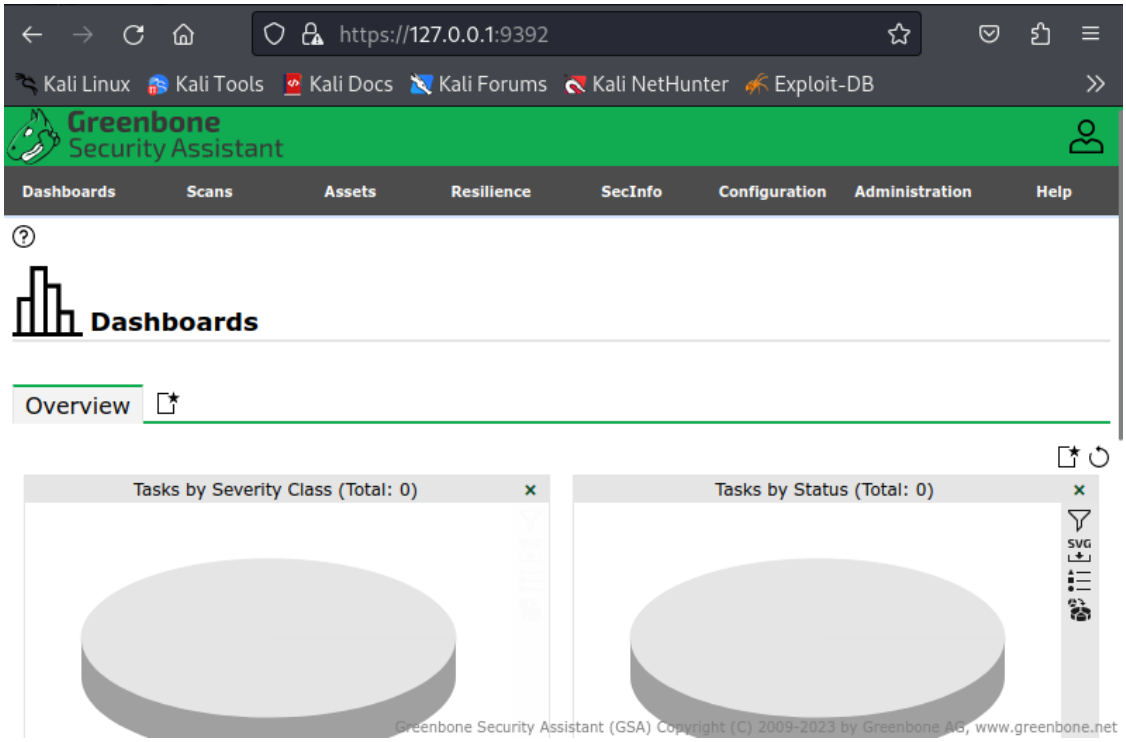

Рисунок 9 – Головна сторінка OpenVAS

Завдання 3. Створення завдання для сканування вразливої інфраструктури.

1. На головній сторінці веб-інтерфейсу GVM обрати пункт меню “Scans” → “Tasks”.

Рисунок 10 – Процес створення нового сканування (вкладки “Scans” – “Tasks”)

2. Перейти до панелі “Task Wizard” для швидкого створення завдання сканування.

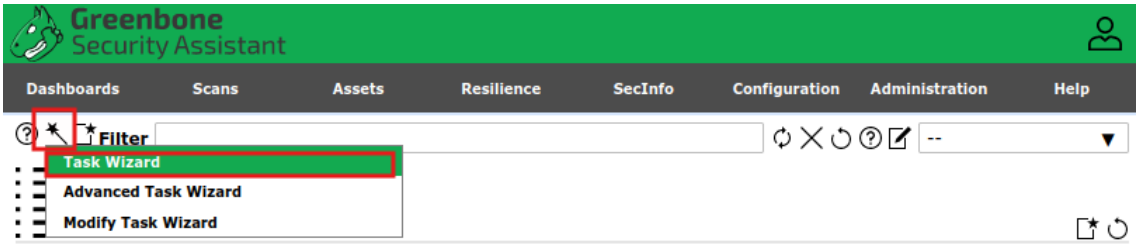

Рисунок 11 – Процес створення нового сканування

В межах віртуальної машини Kali Linux (від Cisco) розгорнуто Docker-контейнер із вразливою інфраструктурою Metasploitable2. IP-адреса вразливого сервера: **172.17.0.2**. Переконатись в доступності цільової системи можна шляхом сканування мережі за допомогою інструмента Nmap.

Metasploitable2 – це спеціалізована лабораторія у вигляді навмисно вразливої операційної системи на базі Linux. Вона використовується для навчання тестуванню на проникнення та аналізу вразливостей.

3. У полі “IP address or hostname” вказати IP-адресу цільового хоста: **172.17.0.2**.

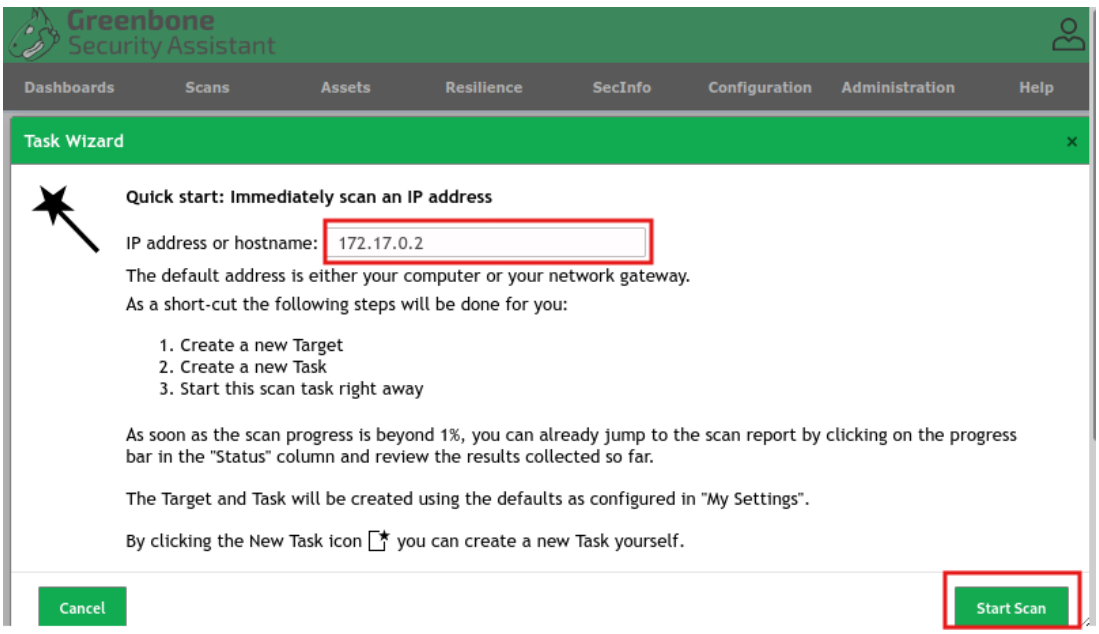

Рисунок 12 – Налаштування параметрів сканування (задання IP-адреси цільової системи)

4. Натиснути ”Start Scan” для запуску процесу сканування.

5. Дочекатися повного завершення перевірки та формування звіту про виявлені вразливості.

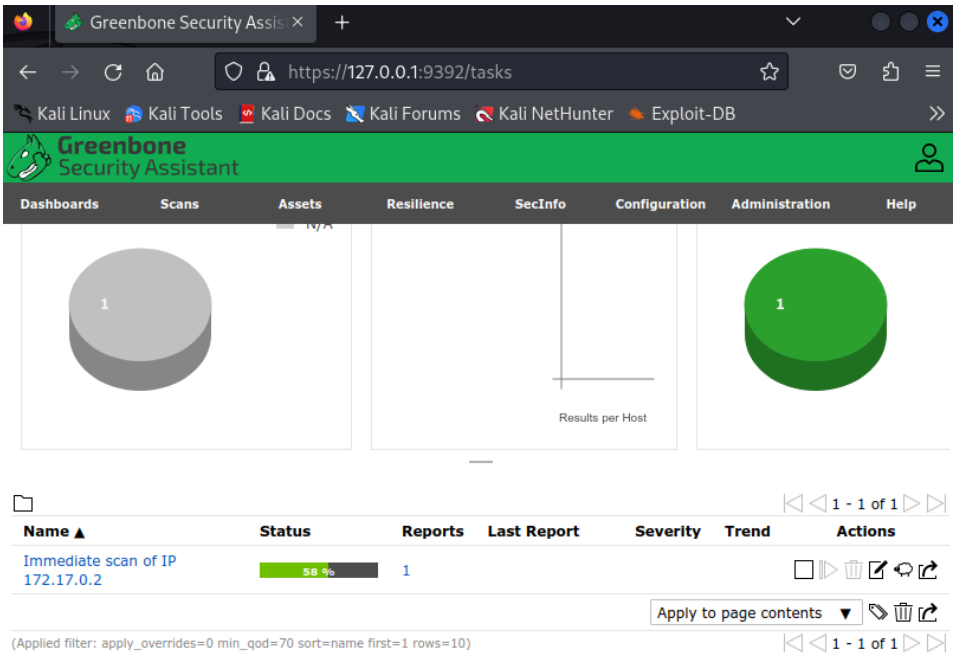

Рисунок 13 – Процес сканування вразливостей на сервері з IP-адресою 172.17.0.2

Завдання 4. Аналіз звіту, створеного в результаті сканування.

1. Відкрити звіт, створений після завершення процесу сканування.

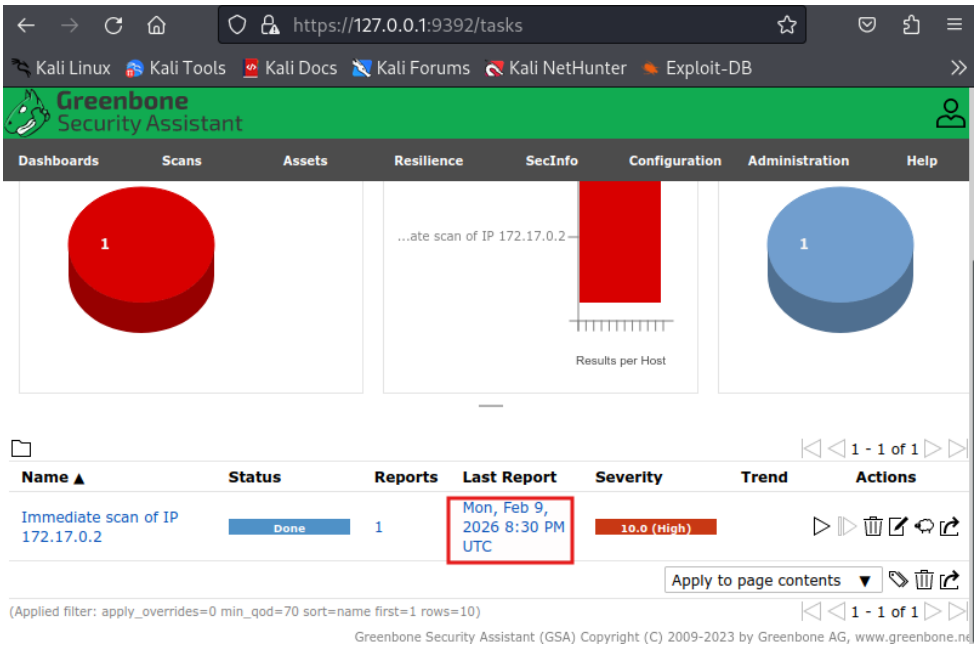

Рисунок 14 – Сформований звіт в результаті сканування вразливостей

2. Проаналізувати всі основні вкладки звіту, зокрема:

- Results – перелік виявлених вразливостей.

- Hosts – інформація про просканові хости.

- Ports – відкриті порти.

- Applications – сервіси.

- Operating Systems – ОС, в межах якої відбувалося сканування.

- CVEs.

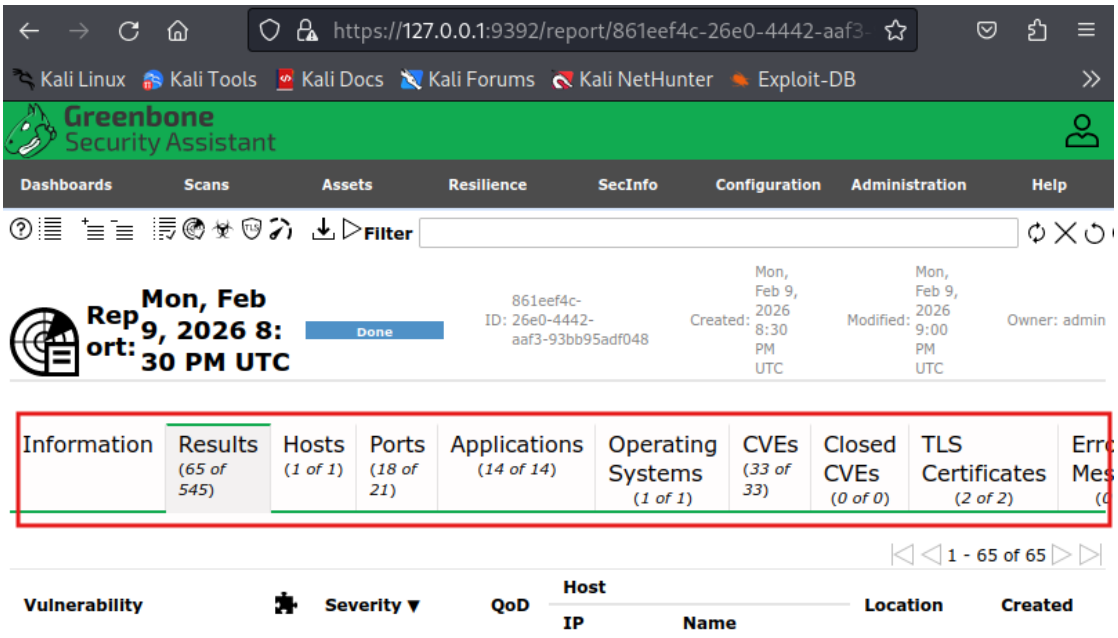

Рисунок 15 – Детальна інформації про результати сканування

3. Визначити вразливості з найвищим рівнем критичності (High/Critical).

4. Для щонайменше двох критичних вразливостей:

- Вказати їхній ідентифікатор CVE.

- Зазначити рівень CVSS.

- Коротко описати суть вразливості.

- Визначити потенційні наслідки її експлуатації.

5. Здійснити пошук додаткової інформації щодо виявлених CVE (п. 4) у відкритих джерелах (наприклад, NIST) та порівняти отримані дані з інформацією у звіті OpenVAS.

6. Зробити висновок щодо загального рівня захищеності досліджуваної системи.

Завдання 5. Ідентифікація сервісів.

1. Використовуючи інструмент Nmap, виконати ідентифікацію сервісів, що працюють на портах, зазначених у звіті OpenVAS (вкладка “Ports”).

nmap -sV -sC 172.17.0.2

2. Проаналізувати отримані результати:

- Встановити назви та версії запущених сервісів.

- Звернути увагу на застарілі або потенційно вразливі версії програмного забезпечення.

Завдання 6. Аналіз виявлених вразливостей.

1. Перейти до розділу “Scans” → “Vulnerabilities” та ознайомитися з переліком виявлених вразливостей на дашборді.

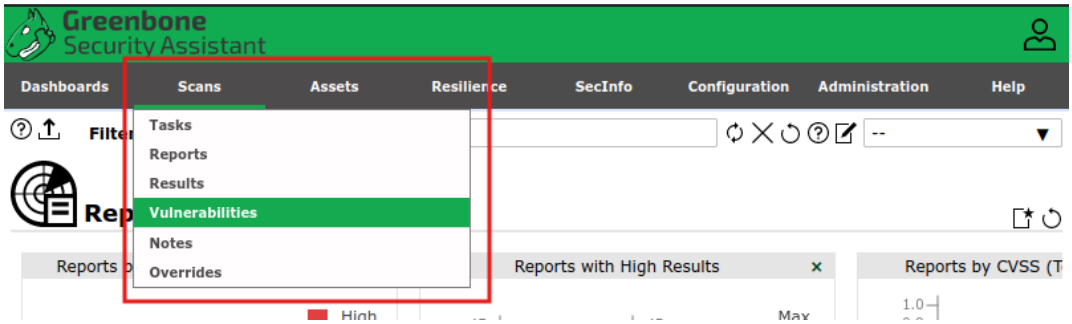

Рисунок 16 – Розділ “Scans”

2. Перейти до розділу “Assets” → “Hosts” / “Operating Systems”.та проаналізувати інформацію про виявлений хост.

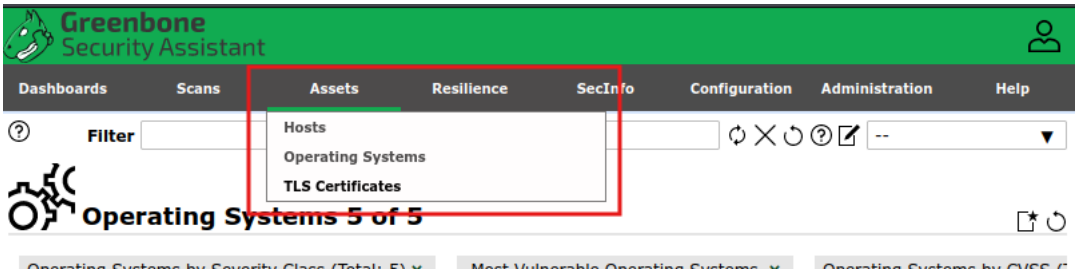

Рисунок 17 – Розділ “Assets”

Контрольні запитання

1. Яке основне призначення інструмента OpenVAS?
2. Який компонент GVM безпосередньо виконує сканування вразливостей?
3. У якому форматі має вигляд ідентифікатор CVE?
4. Що відображається у вкладці “Ports” у звіті OpenVAS?
5. Що означає показник CVSS?
6. Яка команда використовується для запуску служби GVM у Kali Linux?
7. Яке призначення Metasploitable2?

Список джерел

1. Greenbone Vulnerability Management. *HackYourMom*. URL: https://hackyourmom.com/servisy/yak-u-kali-linux-vstanovyty-greenbone-vulnerability-management-kolyshnij-openvas/.
2. OpenVAS. *TryHackMe*. URL: https://tryhackme.com/room/openvas.
3. OpenVAS Cheatsheet. *carmar.is*. URL: https://carmar.is/notes/open-vas-cheatsheet/.