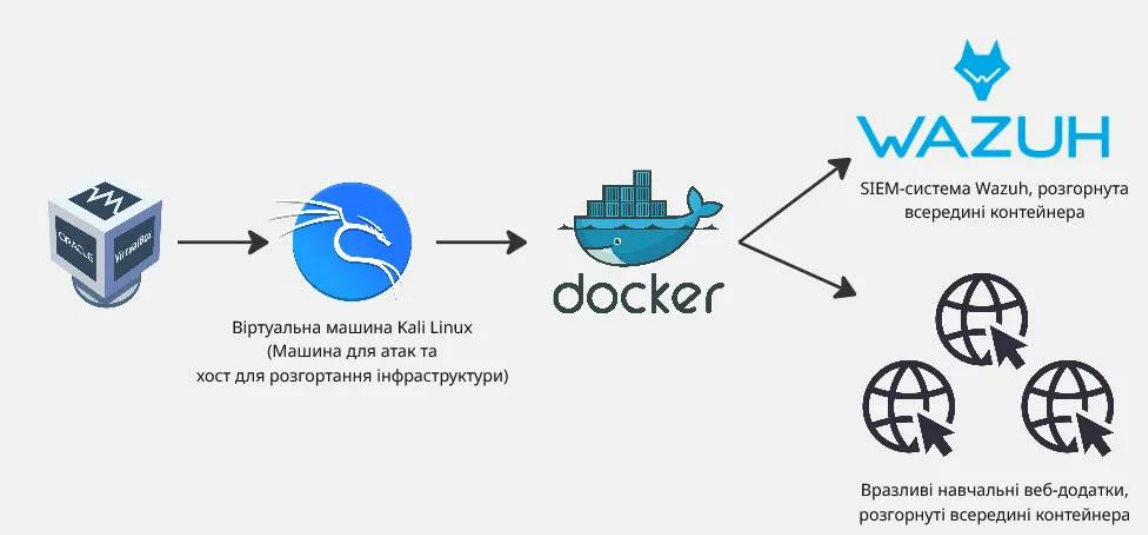
Лабораторна робота №1

Підготовка середовища до виконання практичних робіт з курсу

SOC Analysis Essentials

Загальна схема інфраструктури для виконання лабораторних робіт має наступний вигляд:



На віртуальній машині Kali Linux, яка використовується як машина атакуючого та хост для розгортання інфраструктури, розгортається набір Docker-контейнерів, що містять:

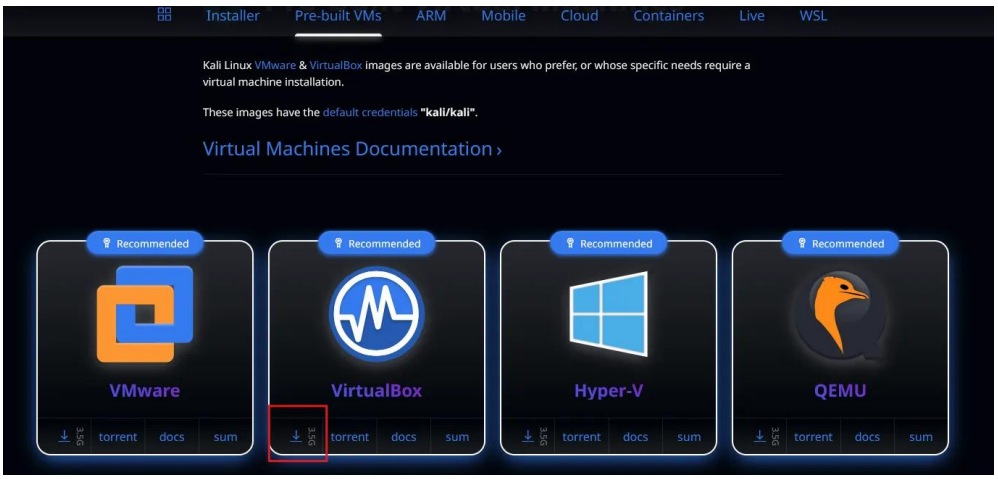
1. SIEM-систему Wazuh для централізованого моніторингу подій безпеки та стану систем.
2. Навчальні вразливі веб-додатки, призначені для відпрацювання практичних навичок аналізу інцидентів та реагування.

Завдання 1. Встановлення образу віртуальної машини Kali Linux.

Посилання на образ:

https://www.kali.org/get-kali/#kali-virtual-machines

На офіційному сайті дистрибутиву Kali Linux необхідно завантажити інсталяційний образ:

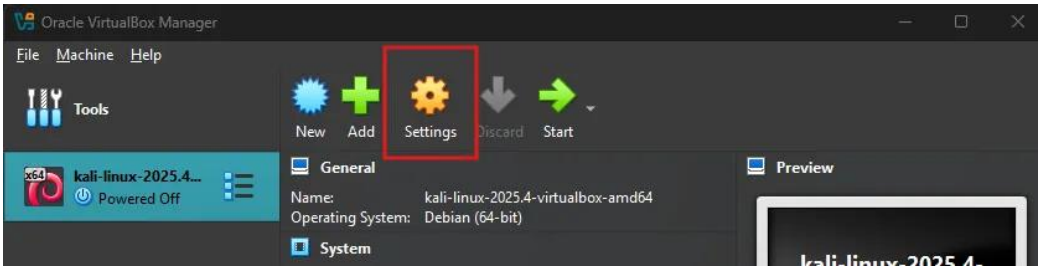


Після успішного завантаження архіву необхідно виконати його розпакування.

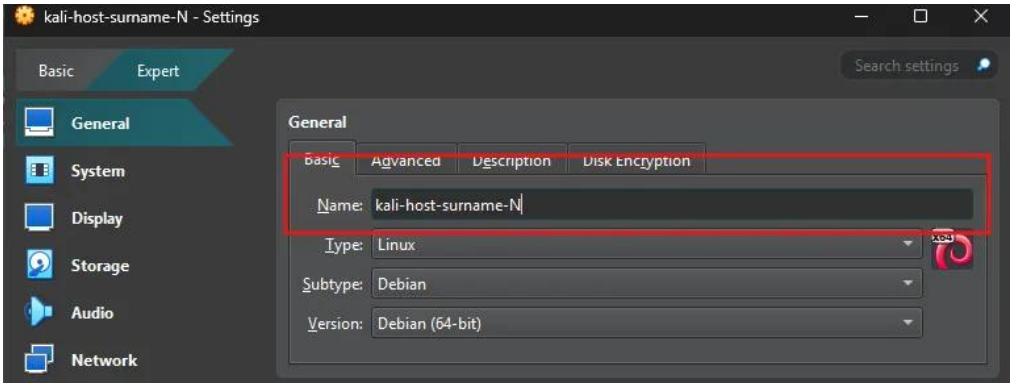
Завдання 2. Встановлення віртуальної машини Kali Linux.

Переходимо до розпакованого архіву та за допомогою подвійного натискання ЛКМ відкриваємо файл «VirtualBox Machine Definition», після чого віртуальна машина автоматично додається до середовища VirtualBox.

Переходимо до налаштувань віртуальної машини Kali Linux.

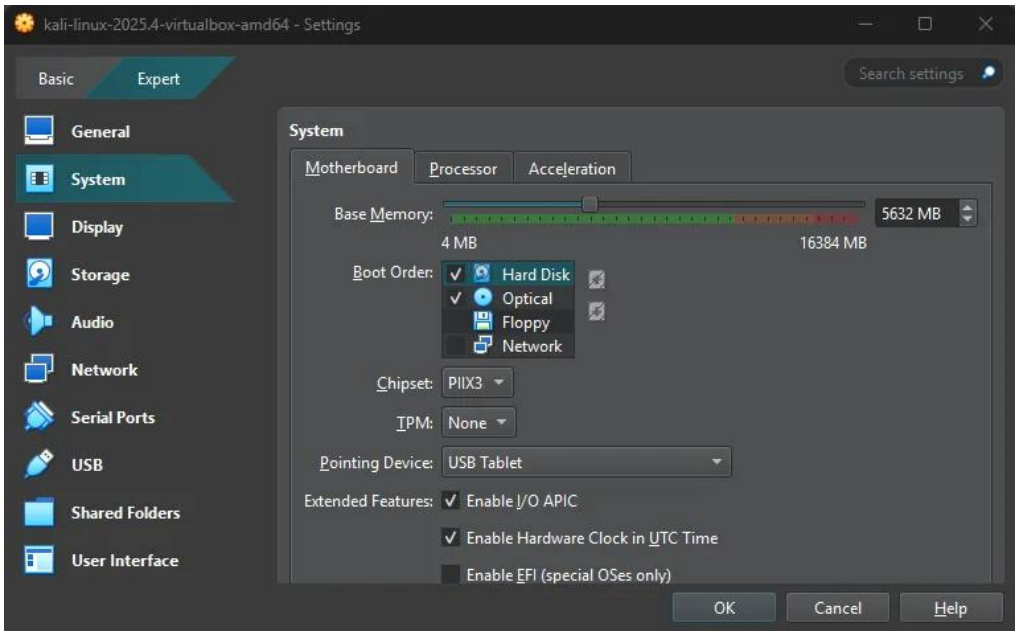


Змінюємо назву віртуальної машини на «kali-host-surname-N», де surname - прізвище, а N - номер варіанту за списком.

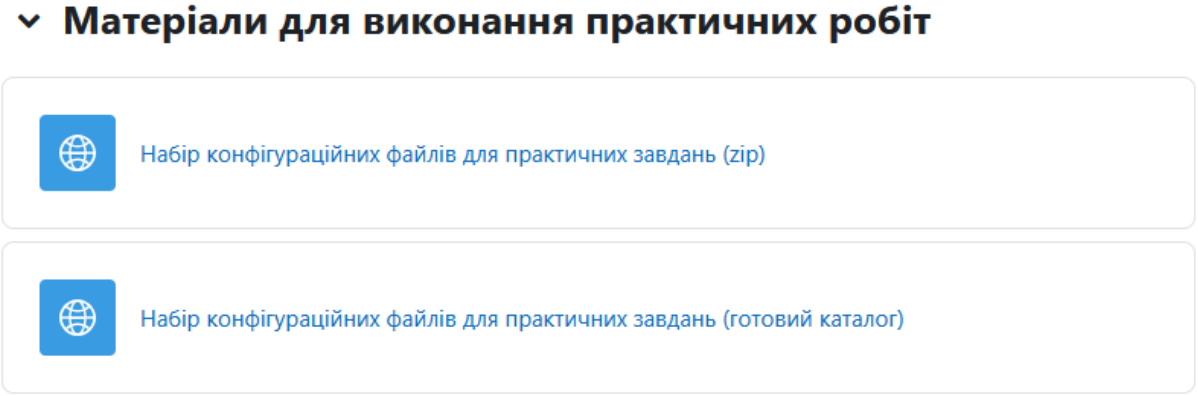


В розділі «System» необхідно встановити значення параметра «Base Memory» у межах 5000 - 5700 МБ, за умови що апаратні характеристики хост-системи це дозволяють.

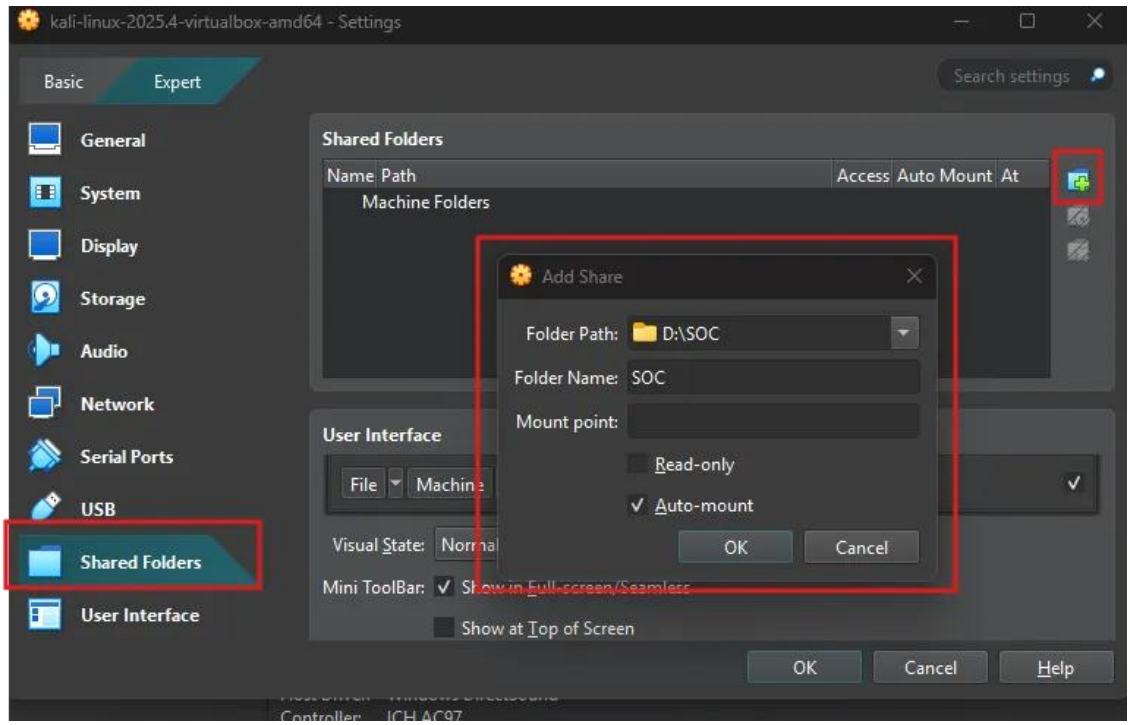
У разі обмеженого обсягу оперативної пам’яті (наприклад, 8 ГБ) допускається встановлення близько 4500 МБ, що є мінімально рекомендованим для коректної роботи віртуальної машини.



У розділі «Shared Folders» необхідно додати директорію, яка містить папку «soc-lab» з усіма матеріалами для виконання лабораторних робіт. Посилання на завантаження папки «soc-lab» знаходиться на порталі (learn.ztu.edu.ua):



Створюємо каталог із назвою «SOC», всередину якого копіюємо папку «soc-lab».



Після підтвердження налаштувань кнопкою «OK» виконуємо запуск віртуальної машини Kali Linux.

Логін: kali

Пароль: kali

Спільний каталог автоматично монтується в каталог */media*. Для зручності роботи його рекомендується скопіювати на робочий стіл:

cd /media

cp -r sf_SOC/ /home/kali/Desktop

cp -r /home/kali/Desktop/sf_SOC/soc-lab/soc-lab/ /home/kali/Desktop/

cd /home/kali/Desktop/soc-lab/

Завдання 3. Встановлення Docker.

 # Крок за кроком виконуємо наступні команди:

 # Створення директорії для зберігання GPG-ключів APT

sudo install -m 0755 -d /etc/apt/keyrings

 # Завантаження офіційного GPG-ключа Docker та конвертація його у формат .gpg

*curl -fsSL https://download.docker.com/linux/debian/gpg | *

sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg

 # Надання прав на читання GPG-ключа для всіх користувачів

sudo chmod a+r /etc/apt/keyrings/docker.gpg

 # Додавання офіційного репозиторію Docker до списку джерел APT

*echo *

*"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] *

*https://download.docker.com/linux/debian bookworm stable" | *

sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

 # Встановлення Docker та Docker Compose з репозиторіїв

sudo apt install -y docker.io docker-compose

 # Перевірка успішного встановлення Docker

docker –version

 # Перевірка встановлення Docker Compose

docker-compose --version

Завдання 4. Розгортання інфраструктури в Docker.

 # Надаємо необхідні права доступу на каталог soc-lab користувачу kali

sudo chown -R $USER:$USER ~/Desktop/soc-lab

sudo chmod -R 775 ~/Desktop/soc-lab

 # Попереднє налаштування Wazuh

sudo ./setup-wazuh.sh

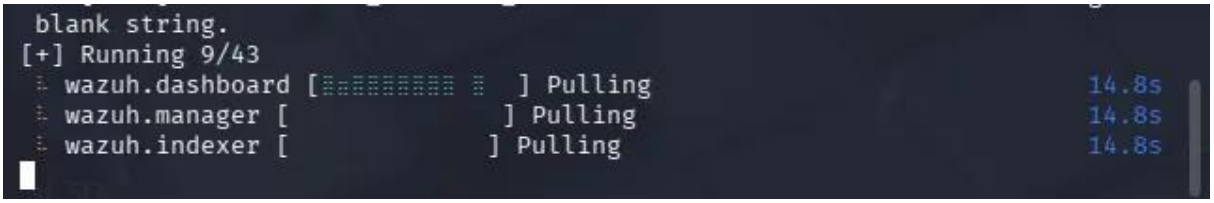
 # Надаємо права на запуск скрипта

sudo chmod +x lab-management.sh

 # Виконуємо розгортання Wazuh в Docker-контейнері

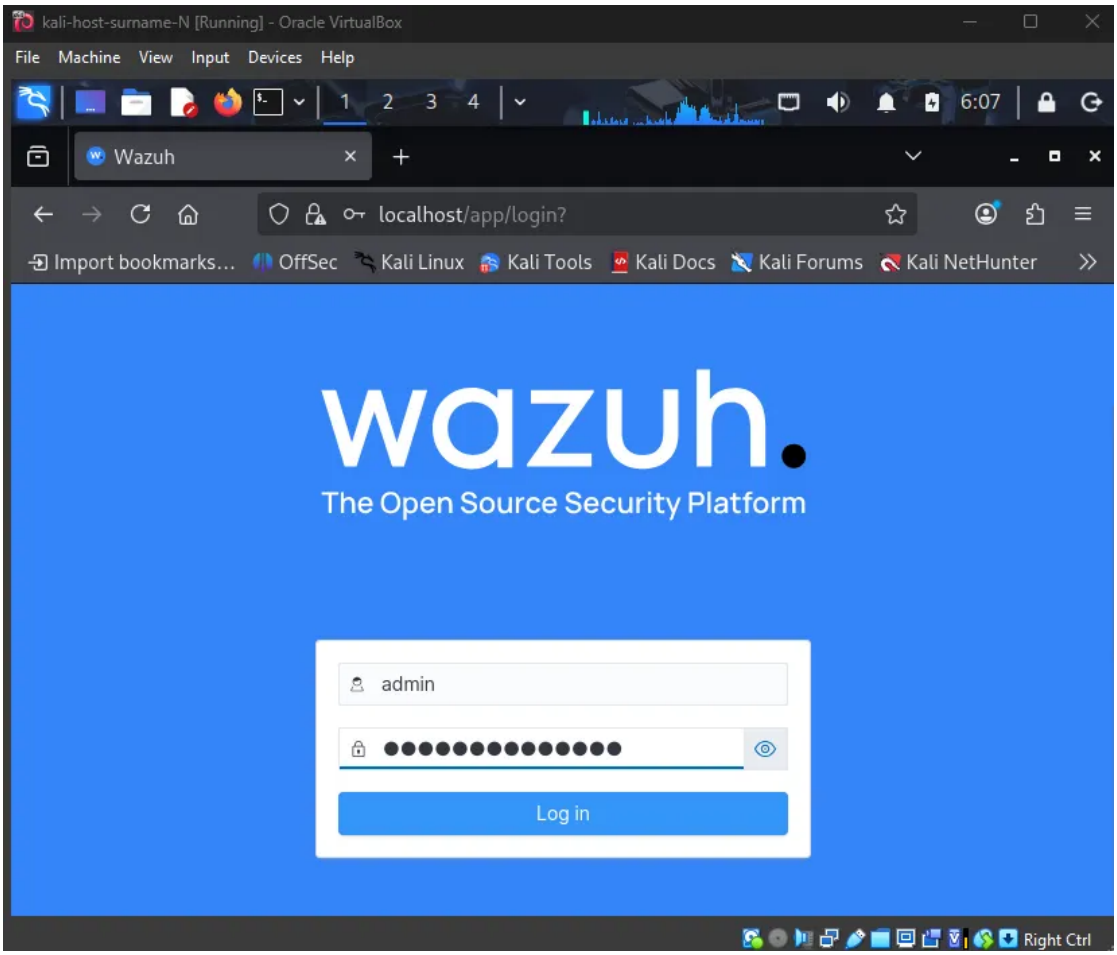
sudo ./lab-management.sh start wazuh

Результат виконання команди *sudo ./lab-management.sh start wazuh*.



Перше розгортання Wazuh всередині Docker-контейнера займає в середньому **до 10 хв.** Для отримання доступу до системи слід у веб-браузері перейти за адресою: **https://localhost**

Приклад розгорнутої SIEM-системи Wazuh всередині Docker-контейнера:

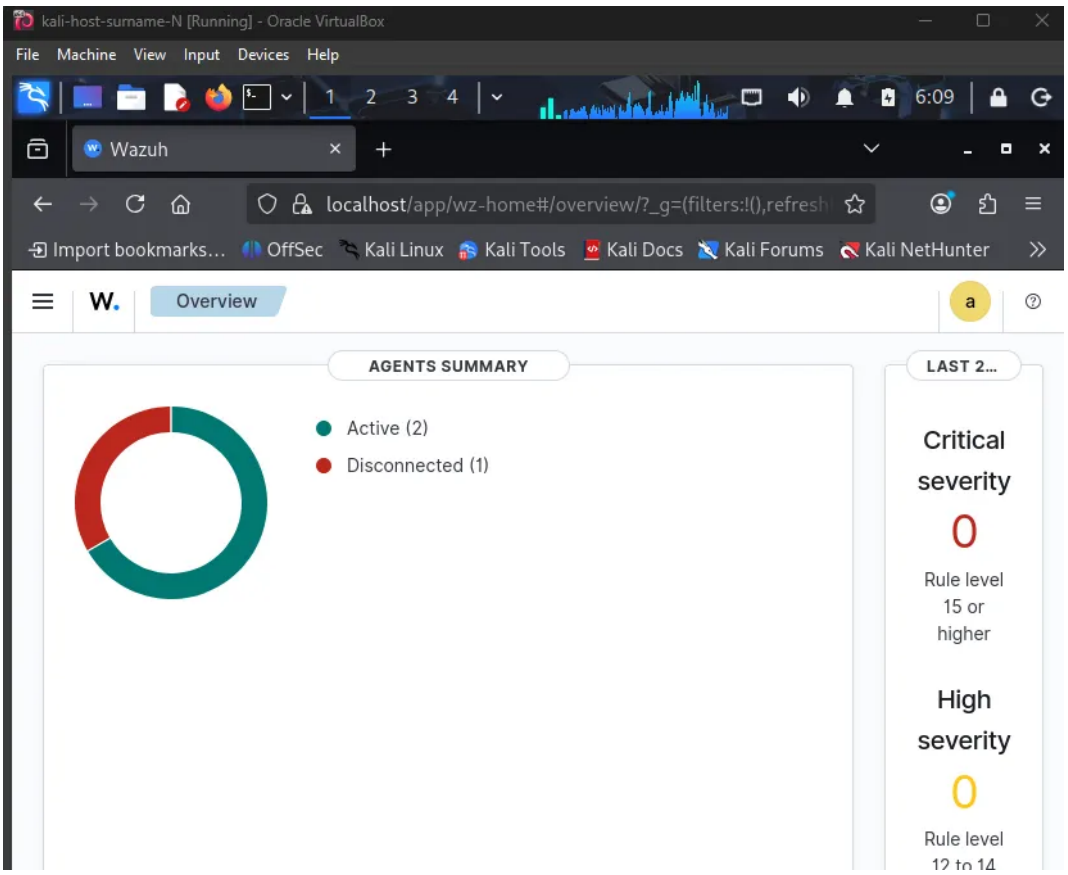


Для доступу до Wazuh:

Логін: admin

Пароль: SecretPassword

Про успішність розгортання Wazuh та агентів свідчить розділ Agents Summary (поле Active). У разі виникнення будь-яких помилок на етапі розгортання Wazuh, слід оновити сторінку за адресою https://localhost:



Завдання 5. Розгортання навчальних вразливих веб-додатків всередині Docker-контейнера.

Для успішного розгортання виконуємо наступну команду:

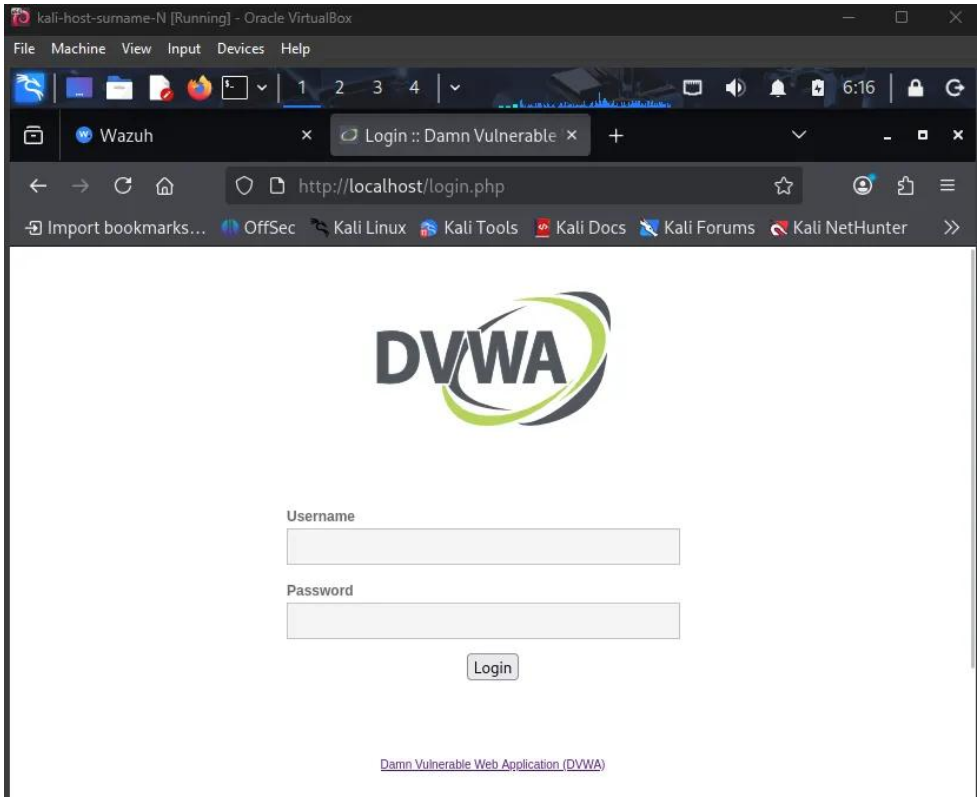
sudo ./lab-management start vuln-lab

Після успішного розгортання веб-додатки будуть доступні за наступними адресами:

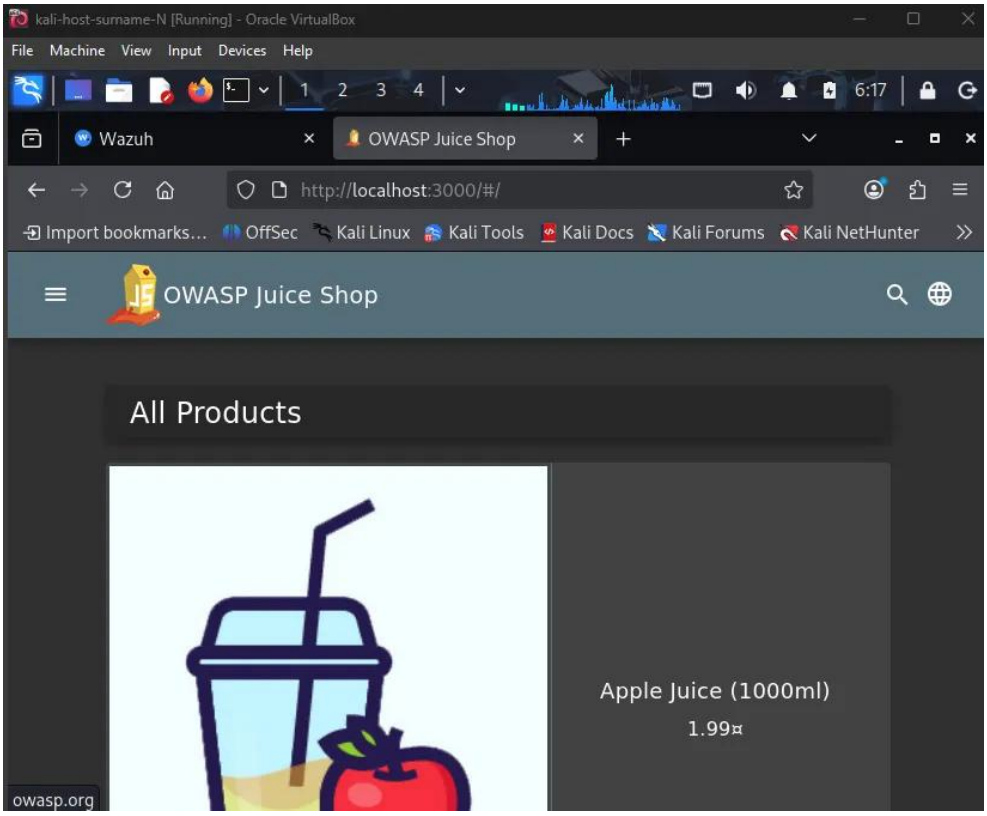
1. DVWA: http://localhost:80 (логін/пароль: admin/password).
2. WebGoat: http://localhost:8080.
3. Juice Shop: http://localhost:3000.
4. NodeGoat: http://localhost:4000.

Найшвидше розгортається веб-додаток DVWA, решта веб-сайтів потребують у середньому близько 5 хвилин для повного запуску. У разі виникнення помилки 404 після розгортання веб-застосунку WebGoat, скріншот розгорнутого веб-сайту можна не додавати до звіту.

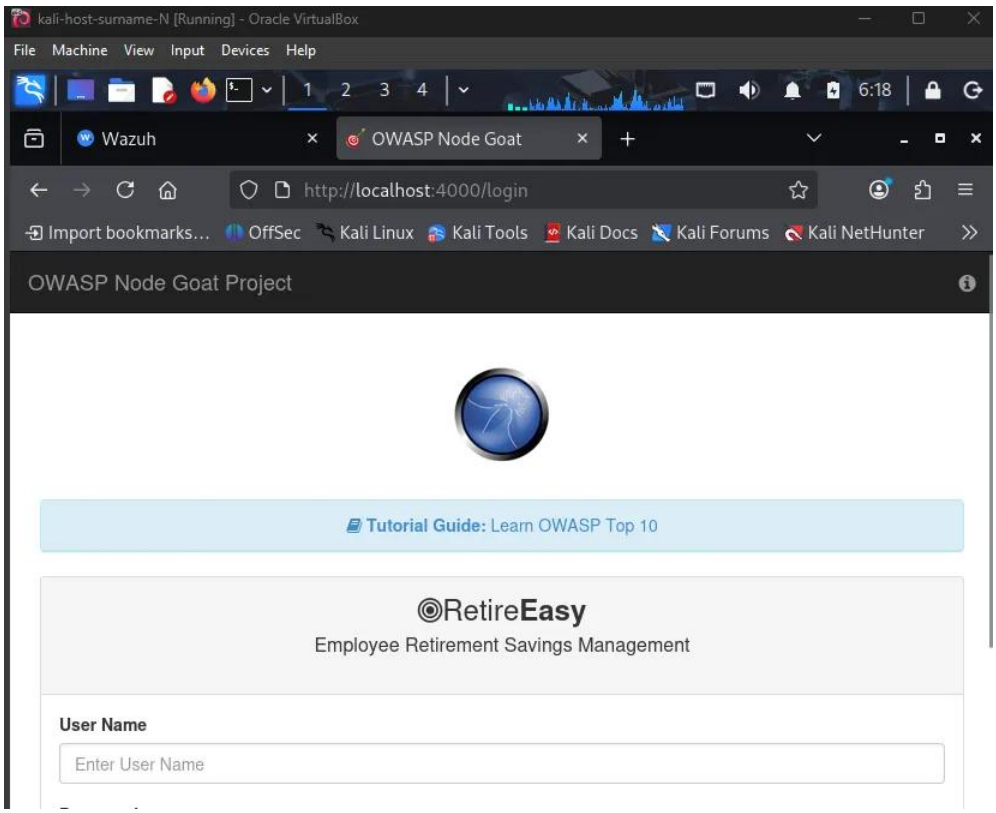
Розгорнутий навчальний веб-сайт DVWA:



Розгорнутий навчальний веб-сайт Juice Shop:



Розгорнутий навчальний веб-сайт Juice Shop:



Для підтвердження успішного розгортання до звіту необхідно додати скріншоти веб-інтерфейсу Wazuh та розгорнутих веб-додатків.