Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Метод підвищення захищеності Docker-контейнерів»

Виконав: студент 2-го курсу, групи 1БС-22м
спеціальності 125 – Кібербезпека
_____ Вячеслав КОЗАЧОК
Керівник: к.т.н., доц., доц. каф. ЗІ
_____ Віталій ЛУКІЧОВ
Опонент: к.т.н., доц., доц. каф . ПЗ
_____ Володимир МАЙДАНЮК
«13» 12 2023 р.

Допущено до захисту

Завідувач кафедри ЗІ
д.т.н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«14» 12 2023 р.

Вінниця ВНТУ – 2023 рік

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти ІІ-й (магістерський)
Галузь знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека
Освітня програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д.т.н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«_19_» _09_____ 2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Козачку Вячеславу Олександровичу

1. Тема роботи: «Метод підвищення захищеності Docker-контейнерів», керівник роботи: Лукічов Віталій Володимирович, к.т.н., доц. каф. ЗІ, затверджені наказом ректора ВНТУ від 18 вересня 2023 року, протокол №247.
2. Строк подання студентом роботи 13 грудня 2023 р.
3. Вихідні дані до роботи:
   - дані зібрані з інтернет-форм, стандартів безпеки. Фактори ризиків ІБ у контейнеризованих середовищах;
   - спосіб реалізації – програма для сканування та виправлення помилок конфігурації Docker-контейнерів.
4. Зміст текстової частини: Вступ. 1. Аналіз інформаційних джерел. 2. Розробка методу підвищення захищеності Docker-контейнерів. 3. Розробка програмного додатку та експериментальне дослідження. 4. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Алгоритм роботи програми(плакат, А4). Рівні середовища Docker(плакат, А4). Схема взаємодії використовуваних компонентів(плакат, А4). Запущені Docker-контейнери для тестування(плакат, А4). Розрахунки приросту коефіцієнту захищеності контейнерів(плакат, А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанти	Підпис, дата	
		завдання видав	виконання прийняв
1	Віталій ЛУКІЧОВ, к.т.н., доц. каф. ЗІ	01.09	10.09
2	Віталій ЛУКІЧОВ к.т.н., доц. каф. ЗІ	01.09	11.10
3	Віталій ЛУКІЧОВ к.т.н., доц. каф. ЗІ	01.09	17.11
4	Ольга РАТУШНЯК., к.т.н., доцент каф. ЕПВМ	01.09	17.11

7. Дата видачі завдання 1 вересня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	01.09.2023 – 10.09.2023	
2	Аналіз літературних джерел за напрямом магістерської кваліфікаційної роботи	10.09.2023 – 15.09.2023	
3	Науково-технічне обґрунтування	16.09.2023 – 22.09.2023	
4	Розробка технічного завдання	23.09.2023 – 29.09.2023	
5	Розробка рішень	30.09.2023 – 12.10.2023	
6	Практична реалізація, моделювання, експериментування, результати	14.10.2023 – 10.11.2023	
7	Розробка розділу економічного обґрунтування доцільності розробки	11.11.23 – 17.11.2023	
8	Аналіз виконання ТЗ, висновки	18.11.2023 – 24.11.2023	
9	Оформлення пояснювальної записки	25.11.2023 – 30.11.2023	
10	Попередній захист та доопрацювання МКР	28.11.2023 – 01.12.2023	
11	Перевірка магістерської роботи на наявність плагіату	02.12.2023 – 10.12.2023	
12	Представлення МКР до захисту	11.12.2023 – 14.12.2023	
13	Захист МКР	14.12.2023 – 21.12.2023	

Студент _____ Вячеслав КОЗАЧОК

Керівник роботи _____ Віталій ЛУКІЧОВ

АНОТАЦІЯ

УДК 004.056

Козачок В. О. Метод підвищення захищеності Docker-контейнерів. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2023. 73 с.

На укр. мові. Бібліогр.: 17 назв; рис.: 19; табл. 14.

Магістерська кваліфікаційна робота присвячена розробці методу, що підвищить захищеність Docker-контейнерів, а також створенню реалізації даного метода програмним шляхом. Для успішної розробки програмного засобу проведено дослідження наявних аналогів програмних реалізацій систем збирання та аналізування. Під час роботи обґрунтовано вибір власних методів, розроблено ряд схем і алгоритмів, здійснено програмну реалізацію. Засіб перевірено на коректність роботи.

Ілюстративна частина складається з 5 плакатів з демонстрацією схеми алгоритму роботи системи та прикладами її використання.

В економічному розділі оцінено витрати на розробку.

Ключові слова: аналіз конфігурації Docker контейнерів, підвищення захищеності Docker контейнерів, автоматизація виправлення помилок

ABSTRACT

Kozachok V. O. A method to increase the security of Docker containers. Master's qualification work in specialty 125 - Cybersecurity, educational program - Security of information and communication systems. Vinnytsia: VNTU, 2023. 73 p.

In Ukrainian. Bibliography: 17 titles; Figures: 19; Table 14.

The master's qualification work is devoted to the development of a method that will increase the security of Docker containers, as well as the creation of a software implementation of this method. For the successful development of the software tool, a study of existing analogues of software implementations of collection and analysis systems was conducted. In the course of the work, the choice of our own methods was substantiated, a number of schemes and algorithms were developed, and the software implementation was carried out. The tool has been tested for correct operation.

The illustrative part consists of 5 posters demonstrating the scheme of the system's algorithm and examples of its use.

The economic section estimates the development costs.

Keywords: analysis of Docker container configuration, increasing the security of Docker containers, automation of error correction.

ЗМІСТ

ВСТУП

В епоху швидкого технологічного розвитку повсюдне поширення технологій контейнеризації зробило революцію в розробці, розгортанні та масштабуванні додатків. Docker, провідний лідер в управлінні контейнерами, надає потужну основу для інкапсуляції додатків та їх залежностей. Однак, з повсюдним впровадженням контейнерних рішень, проблеми з безпекою стають все більш актуальними. Забезпечення відмовостійкої та безпечної конфігурації контейнерів Docker стає першочерговим завданням, що вимагає надійних рішень для автоматизації.

Магістерська кваліфікаційна робота заглиблюється в інтеграцію Docker і Ansible, орієнтовану на безпеку, і досліджує, як об'єднані сили цих технологій можуть зміцнити контейнерні середовища. Оскільки організації стикаються з необхідністю захисту своїх додатків та даних, роль Ansible стає ключовим інструментом для організації безпечних конфігурацій та впровадження стандартів відповідності в інфраструктурах, побудованих на Docker.

Дослідження намагається розгадати тонкощі цієї інтеграції, ретельно вивчаючи перетин Docker та Ansible з точки зору безпеки. Шляхом всебічного аналізу найкращих практик безпеки, стратегій зменшення ризиків та практичних прикладів використання, ця робота має на меті надати фахівцям з безпеки та особам, які приймають рішення в IT, знання та інструменти, необхідні для створення надійної системи безпеки в їхніх контейнерних екосистемах.

Починаючи з вивчення основних функцій безпеки Docker і Ansible, це дослідження формулює їх індивідуальний внесок у захист контейнерних середовищ. Згодом фокус зміщується на точки інтеграції, де Ansible розширює можливості безпеки Docker, автоматизуючи конфігурацію засобів контролю безпеки, управління доступом і перевірку відповідності.

Завдяки аналізу реальних інцидентів безпеки, моделюванню загроз та практичним сценаріям впровадження, ця робота має на меті надати читачам всебічне розуміння того, як Ansible може бути використаний для підвищення

безпеки контейнерів Docker. Вона розглядає динамічний ландшафт проблем безпеки в контейнерних середовищах і надає прагматичні поради щодо захисту робочих процесів оркестрування контейнерів.

Оскільки безпека залишається наріжним каменем у цифровій сфері, ця робота слугує посібником для фахівців з безпеки та IT-спеціалістів, які орієнтуються у складному середовищі інтеграції Docker та Ansible. Наступні розділи заглиблюються в нюанси захисту контейнерів Docker, пропонуючи практичні стратегії для зменшення ризиків, впровадження безпечних конфігурацій та забезпечення відповідності вимогам в рамках контейнерних інфраструктур.

Метою є підвищення захищеності Docker-контейнерів та їх середовища.

Об’єктом дослідження є процес сканування та автоматизації виправлення помилок конфігурації контейнерів.

Предметом дослідження є система віддаленої конфігурації Docker контейнерів та віддалених машин.

Наукова новизна магістерської роботи полягає в подальшому розвитку методу сканування та виправлення помилок конфігурації у Docker-контейнерах за допомогою Ansible.

Результати здійснених досліджень під час виконання магістерської кваліфікаційної роботи будуть доповідатись на Міжнародній науково-практичній конференції студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи».

1 АНАЛІЗ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1.1 Науково-технічне обґрунтування розробки аналізу Docker середовища на вразливості.

Docker-контейнери – це легкі, портативні та самодостатні одиниці, які інкапсулюють програму та її залежності, включаючи бібліотеки, середовище виконання та системні інструменти. Ці контейнери забезпечують узгоджене та відтворюване середовище в різних обчислювальних середовищах, що дозволяє розробникам безперешкодно створювати, постачати та запускати додатки на різних платформах. До ключових особливостей контейнерів Docker належать ізоляція, переносимість, ефективність, керування версіями, реєстр образів, оркестрування [1].

В сучасному світі доводиться впроваджувати множину засобів, для забезпечення інфраструктури. Використання контейнерів хоч і зменшує кількість вразливостей з одного боку, проте дає зловмисникам нові вектори атак, які можна експлуатувати. Починаючи від рівня серверного обладнання та операційної системи, закінчуючи двигуном контейнерів, засобом управління контейнерами, середою виконання і власне самим контейнером рис. 1.1.

Контейнери використовують віртуалізацію на рівні операційної системи, щоб ізолювати програми від базової інфраструктури. Ця ізоляція гарантує, що програми працюють стабільно, незалежно від хост-середовища.

Docker контейнери пакують додатки та їхні залежності в єдиний стандартизований блок, це забезпечує їх переносимість. Тобто контейнер може працювати на будь-якій системі, що підтримує Docker, що полегшує переміщення додатків між середовищами розробки, тестування та виробництва.

Контейнери використовують ядро операційної системи хоста, зменшуючи накладні витрати, пов'язані з традиційною віртуалізацією, що забезпечує

ефективність. Це призводить до більш швидкого запуску та більш ефективного використання ресурсів.

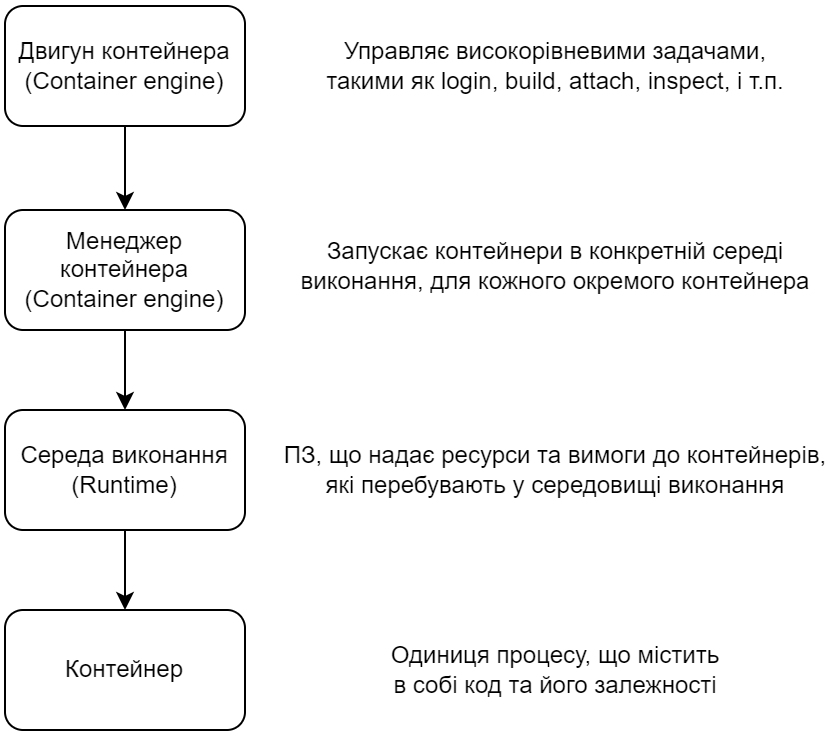


Рисунок 1.1 – Рівні середовища Docker

Docker використовує образи, які є знімками файлової системи та конфігурації контейнера. Ці образи можна версіонувати, надавати спільний доступ та зберігати у реєстрах, що полегшує спільну роботу та розповсюдження програм. Цей принцип Docker має назву “керування версіями та реєстр образів”.

Оркестрація досягається за допомогою таких інструментів, як Kubernetes або Docker Swarm, що дозволяє керувати великомасштабними розгортаннями, балансуванням навантаження та автоматичним масштабуванням, часто згадується як оркестрування.

Загалом, контейнери Docker революціонізували спосіб розробки, розгортання та управління програмним забезпеченням, забезпечивши узгоджене та ізольоване середовище для додатків, спростивши процес розробки та покращивши масштабованість і надійність розгортання програмного забезпечення.

1.2 Способи для впровадження безпеки

Безпека в контейнерних середовищах має першорядне значення через унікальні характеристики контейнерної технології та динамічний характер розгортання сучасних додатків.

Ізоляція та багатокористувацьке використання дозволяють контейнерам використовувати ядро операційної системи хоста, і без належної ізоляції один скомпрометований контейнер може потенційно вплинути на інші на тому ж хості. Забезпечення надійних механізмів ізоляції має вирішальне значення для запобігання порушенням безпеки та захисту конфіденційних даних [2].

Контейнерні програми будуються з образів, які слугують шаблоном для контейнерів. Забезпечення безпеки цих зображень є надзвичайно важливим. Це передбачає регулярне сканування на наявність вразливостей, використання надійних базових образів та ведення безпечного реєстру образів.

Моніторинг та захист контейнерів під час виконання є важливими аспектами безпеки контейнерів. Сюди входить виявлення загроз у реальному часі, сканування вразливостей та забезпечення запуску контейнерів з найменшими привілеями, необхідними для виконання їхніх функцій.

Контейнери взаємодіють один з одним і з зовнішніми сервісами через мережі. Впровадження заходів мережевої безпеки, таких як сегментація мережі, брандмауери та шифрування, має дуже велике значення для захисту даних під час передачі та запобігання несанкціонованому доступу.

Регулярне оновлення та виправлення як хост-системи, так і контейнерних додатків є життєво важливим. Це допомагає усунути відомі вразливості та гарантує, що все контейнерне середовище залишається безпечним протягом тривалого часу.

Таким чином, важливість безпеки в контейнерних середовищах обумовлена необхідністю захисту від особливих та виключних викликів, що виникають завдяки контейнерним технологіям. Для побудови і підтримки безпечної контейнерної

інфраструктури необхідний цілісний підхід, що охоплює безпеку зображень, захист під час виконання, мережеву безпеку і відповідність нормативним вимогам.

Docker має вбудовані засоби безпеки, які допомагають створити безпечне середовище контейнеризації, які допомагають захистити Docker від більшості загроз. Розглянемо їх більш детально.

Docker використовує простори імен Linux для забезпечення ізоляції процесів. Простори імен розділяють різні системні ресурси, такі як процеси, мережа і файлові системи, між контейнерами, гарантуючи, що кожен контейнер працює у власному просторі імен і не має видимості або доступу до ресурсів інших контейнерів.

Docker використовує cgroups для керування та обмеження системних ресурсів, таких як процесор, пам'ять та дисковий ввід/вивід, для кожного контейнера. Це запобігає надмірному споживанню контейнерами ресурсів і допомагає забезпечити справедливий розподіл ресурсів у хост-системі.

Docker використовує багаторівневу файлову систему для образів контейнерів. Кожен рівень представляє певний набір змін у файловій системі. Така архітектура дозволяє повторно використовувати образи і ділитися ними. Образи Docker можна підписувати і перевіряти, що підвищує їх цілісність і безпеку.

Docker підтримує використання файлових систем тільки для читання в контейнерах. Це обмежує можливості процесів всередині контейнера вносити зміни до файлової системи, підвищуючи безпеку, запобігаючи несанкціонованим модифікаціям.

Простори імен користувачів у Docker дозволяють зіставляти користувачів контейнера з непривілейованими користувачами на хості, зменшуючи ризик, пов'язаний з виходом контейнера з-під контролю. Ця функція допомагає зменшити вплив потенційних вразливостей безпеки під час виконання контейнера.

Docker дозволяє використовувати Seccomp (режим безпечних обчислень) для обмеження системних викликів, доступних для контейнера. Це допомагає мінімізувати поверхню атаки контейнера, дозволяючи лише певний набір системних викликів, зменшуючи ризик використання вразливостей на рівні ядра.

Docker Content Trust забезпечує цілісність та автентичність зображень. Він використовує цифрові підписи для підпису зображень, що дозволяє користувачам перевіряти видавця та цілісність зображення перед тим, як витягнути та запустити його.

Docker забезпечує мережеву ізоляцію, щоб запобігти безпосередньому спілкуванню контейнерів між собою, якщо це явно не налаштовано. Це допомагає контролювати і захищати зв'язок між контейнерами і зовнішньою мережею.

1.3 Вбудовані засоби підвищення захищеності середовища

Перший вбудований механізм, що буде розглянуто, це принцип найнижчих привілеїв. Демон Docker забезпечує режим rootless користувача, також відомий як "режим без прав root" [3]. Режим без прав root не потребує привілеїв адміністратора ані для запуску демонів Docker, ані для запуску контейнерів. Це дуже важлива особливість, яку завжди слід враховувати. Вона зменшує будь-які вразливості в демоні Docker і в процесах виконання контейнерів. Основний принцип полягає у тому, що у режимі без привілеїв користувача root будь-який процес Docker виконується у просторі імен користувача.

Спробуємо встановити rootless доступ на власній машині:

```
ubuntu@ip-172-31-93-29:~$ /usr/bin/dockerd-rootless-setuptool.sh install
[INFO] Creating /home/ubuntu/.config/systemd/user/docker.service
[INFO] starting systemd service docker.service
…
[INFO] Installed docker.service successfully.
[INFO] To control docker.service, run: `systemctl --user (start|stop|restart) docker.service`
[INFO] To run docker.service on system startup, run: `sudo loginctl enable-linger ubuntu`

[INFO] Creating CLI context "rootless"
Successfully created context "rootless"
[INFO] Using CLI context "rootless"
Current context is now "rootless"

[INFO] Make sure the following environment variable(s) are set (or add them to ~/.bashrc):
export PATH=/usr/bin:$PATH

[INFO] Some applications may require the following environment variable too:
export DOCKER_HOST=unix:///run/user/1000/docker.sock
```

Обов’язково треба встановити змінні оточення

```
ubuntu@ip-172-31-93-29:~$ export PATH=/usr/bin:$PATH
ubuntu@ip-172-31-93-29:~$ export DOCKER_HOST=unix:///run/user/1000/docker.sock
```

Ось так відпрацьовує команда запуску nginx без встановленого rootless доступу:

```
ubuntu@ip-172-31-90-191:~$ docker run -d --name nginx nginx
docker: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock:
Post "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/create?name=nginx": dial unix /var/run/docker.sock: connect: permission denied.
```

Друге, що буде розглянуто це управління ресурсів у Docker контейнерах.

Згідно з дизайном Docker, контейнери не мають обмежень на апаратні ресурси, які вони можуть використовувати; ось чому підтримка функцій Linux Cgroups є важливою. Безпека апаратного забезпечення та хостової ОС. Причина такого вибору очевидна: контейнер не знає, який сервіс або додаток буде запущено, тому він не зможе передбачити кількість ресурсів, які буде виділено для виконання конкретного завдання. Такий механізм досяжний лише у комплексних середовищах, де використовується штучний інтелект або передові методології управління.

Якщо контейнер скомпрометований, зловмисник може використовувати всі апаратні ресурси, які може надати механізм контейнера, якщо втеча з контейнера успішна, зловмисник може отримати доступ до основних ресурсів хоста, що може призвести до латеральних переміщень і компрометації мережі. Гарною практикою є встановлення квоти ресурсів для контейнерів, щоб встановити обмеження на ресурси там, де вони відсутні за замовчуванням. Багато з цих можливостей безпосередньо пов'язано з можливостями ядра Linux.

Ресурс пам'яті є одним з двох обчислювальних ресурсів, які є надзвичайно важливими; відсутність обмеження може призвести до виникнення такого виключення як Out Of Memory Exception (OOME), що потенційно може призвести до зупинки машини. Docker може встановлювати обмеження пам'яті, які дозволяють контейнеру споживати лише виділену пам'ять і не більше. Така

методологія також відома як жорстке обмеження. Крім того, Docker може дозволити контейнеру споживати стільки пам'яті, скільки йому потрібно, але тільки якщо виконуються певні умови, також відомі як м'яке обмеження (soft limit).

Ресурс центрального процесора є другим важливим фактором при розгляді обчислювальних ресурсів. Аналогічно, за дизайном Docker, доступ контейнерів до ресурсів центрального процесора хост-машини є потенційно необмеженим. Існує два способи налаштувати обмеження ресурсів центрального процесора для контейнерів:

– Планувальник CFS
– Планувальник реального часу (Realtime scheduler)

Планувальник повністю справедливого розподілу ресурсів (CFS) - це функція ядра Linux, яка розподіляє та обробляє ресурси процесора для виконання процесів. Основною метою CFS є максимізація загальної ефективності роботи процесора з точки зору обробки процесів. Параметри CFS, Docker може змінювати налаштування Cgroups для контейнерів за допомогою наступних прапорців:

Пропонується застосувати сценарій безпеки до використання планувальника CFS [4]. У сценарії, коли хост має лише 1 процесор, контейнер може, залежно від програми, яку він обслуговує, споживати набагато більше процесорних циклів, ніж хост, на якому він знаходиться. Це може призвести до нестабільної роботи хоста і, врешті-решт, до аварійного завершення роботи або до зловживань з боку зловмисника. З огляду на це, контейнеру щосекунди виділяється максимум 50% процесорних ресурсів, що зберігає стабільність роботи хоста:

Приклад команди для обмеження кількості CPU для Docker контейнера.

```
docker run -it --cpu-period=100000 --cpu-quota=50000 debian /bin/bash
```

1.4 Вразливості Docker контейнерів

Докерні контейнери, надаючи численні переваги, також створюють унікальні проблеми з безпекою. Розуміння цих загальних загроз безпеці має важливе значення для ефективного захисту контейнерних середовищ. Перед тим як ми розглянемо вразливості контейнерів, буде доречно згадати, що у 2020 році команда

з кібербезпеки Aqua Security виявила новий метод, за допомогою якого зловмисники створювали шкідливі образи безпосередньо на неправильно налаштованих хостах [5]. Представлені дослідницькі групи виступають за "динамічне сканування", яке було проведено в рамках цього дослідження, щоб виявити приховані загрози, які пропускаються при статичному аналізі вразливостей. Аналіз Prevasio, який проводився на 800 машинах протягом місяця, показав, що контейнери, запущені з багатьох підозрілих зображень, завантажували і виконували шкідливе програмне забезпечення табл. 1.1. Табличні дані можна представити у вигляді діаграми, які представлені на рис. 1.2. Дослідники запустили антивірус Clam проти шкідливого програмного забезпечення, виявленого під час виконання, та сканер вразливостей Trivy від Aqua Security.

Таблиця 1.1 – Статистика заражень образів Docker-контейнерів

Назва ШПЗ	Кількість заражених контейнерів	Кількість завантажень заражених контейнерів
Майнери	2842 (44%)	129.5M
Утиліти для зламу	1269 (20%)	70M
ШПЗ для Windows	413 (6.4%)	575K
Викрадач біткоїн-гаманців	1482 (23%)	95M
Інше ШПЗ	426 (6.6%)	9.7M

Треба підкреслити, що саме через неправильно налаштовані контейнери і виникає загроза зламу, тому треба більше приділяти часу правильній конфігурації контейнерного середовища. Адже саме через неправильну конфігурацію у контейнерах, можуть з’явитися ключові загрози безпеці, характерні для Docker.

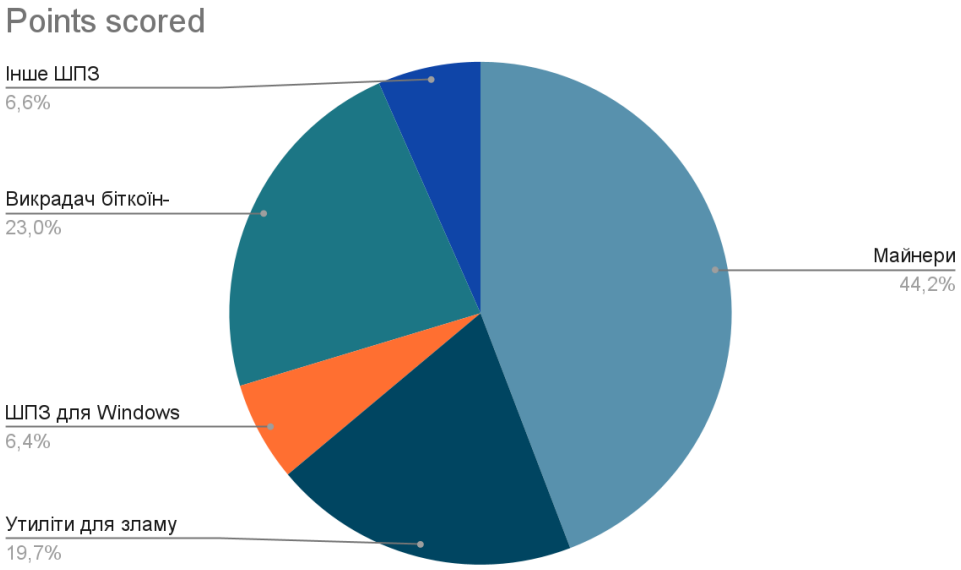


Рисунок 1.2 – Діаграма розподілення типів ШПЗ у образах Docker-контейнерів

Наприклад втеча з контейнера, яка означає, що зловмисник виходить за межі ізоляції контейнера і отримує несанкціонований доступ до основної хост-системи. Використання просторів імен користувачів та регулярне оновлення операційної системи і демону Docker, а також впровадження суворих принципів найменших привілеїв в контейнерах, щоб мінімізувати вплив успішних виходів з контейнера.

Ескалація привілеїв передбачає отримання зловмисником підвищених дозволів всередині контейнера, що потенційно може призвести до несанкціонованого доступу або маніпуляцій з ресурсами. Щоб знизити ризик необхідно використовувати принципи мінімальних привілеїв, запускаючи контейнери в просторів імен користувачів, що не мають прав root. Також необхідно уникати надання зайвих привілеїв процесам, що працюють у контейнерах [6].

Вагомою проблемою стає використання незахищених або скомпрометованих образів контейнерів може призвести до появи вразливостей у середовищі, що потенційно може призвести до експлуатації та компрометації. В якості заходів що можна вжити для зменшення ризику можна розглядати такі варіанти, як регулярну перевірку образів на наявність вразливостей за допомогою інструментів сканування безпеки, використання надійних базових образів.

Особливо часто розробники ПЗ неправильно розпоряджаються із секретами, що використовуються у Docker контейнерах. Зберігання конфіденційної інформації, такої як паролі або ключі API, у вигляді простого тексту в образах Docker або змінних середовища контейнера може призвести до несанкціонованого доступу до критично важливих даних. Для зменшення подібних інцидентів, необхідно використовувати інструменти оркестрування або безпечні рішення, такі як Docker Secrets, для керування та захисту конфіденційної інформації. Необхідно уникати вставлення секретів безпосередньо в Docker-файлах або змінних середовища, а також ні в якому разі не зберігати конфіденційні дані у git репозиторіях.

Недостатня мережева безпека також може стати вектором атаки зловмисників. Незахищені мережеві конфігурації можуть призвести до несанкціонованого доступу до контейнерів або підслуховування, особливо в архітектурах з декількома контейнерами або мікросервісами. Захиститися від цього допомагає впровадження сегментації мережі, використання брандмауерів для контролю трафіку між контейнерами та захищені оверлейні мереж для зв'язку між контейнерами.

Відсутність комплексної реєстрації та моніторингу може перешкоджати виявленню інцидентів безпеки, що ускладнює ідентифікацію та реагування на потенційні загрози. Тому треба впроваджувати найкращі практики ведення журналів, використовувати централізовані рішення для ведення журналів і налаштувати надійний моніторинг для контейнерних середовищ, щоб виявляти події безпеки та реагувати на них.

Зловмисники можуть скомпрометувати реєстри зображень контейнерів, що призведе до поширення шкідливих зображень, які можуть бути мимоволі завантажені користувачами. Використання довірених, автентифікованих реєстрів, підписання та перевірка образів, перевірка образів, отримані з реєстрів, на цілісність, забезпечить вас найновішими і безпечними образами контейнерів.

Невиправлене програмне забезпечення та залежності, якщо регулярно не оновлювати, може бути вразливими до відомих вразливостей у системі безпеки. Рішенням є регулярне оновлення та використання базових образів, а також впровадження процес моніторингу та своєчасне застосування патчів безпеки.

Усунення цих загроз передбачає поєднання безпечної конфігурації, регулярного моніторингу та дотримання найкращих практик безпеки. Дуже важливо бути в курсі нових загроз і впроваджувати стратегію глибокого захисту, щоб зменшити ризики, пов'язані з використанням контейнерних середовищ Docker. Захист контейнерів Docker передбачає застосування комбінації методів, які стосуються різних аспектів контейнеризації, включаючи безпеку образів, безпеку під час виконання, мережеву безпеку та загальну інфраструктуру. Далі буде наведено комплексний набір найкращих практик безпеки для контейнерів Docker.

Використовуйте інструменти сканування образів для виявлення та усунення вразливостей в образах контейнерів перед їх розгортанням. Зменшуйте кількість шарів в образах, щоб мінімізувати поверхню атаки і підвищити ефективність. Створюйте образи лише з необхідними залежностями та компонентами, мінімізуючи ризик вразливостей безпеки. Видаляйте непотрібні інструменти та утиліти з кінцевого образу, щоб зменшити ризик експлуатації.

Запускайте контейнери від імені користувачів, які не є користувачами root, щоб зменшити вплив порушень безпеки та обмежити потенційну ескалацію привілеїв.

Використовуйте простори імен користувачів для зіставлення ідентифікаторів користувачів контейнера з ідентифікаторами непривілейованих користувачів на хості, що підвищує безпеку.

Встановлюйте ліміт ресурсів за допомогою cgroups, щоб запобігти надмірному споживанню контейнерами процесора, пам'яті та інших ресурсів.

Також використовуйте мережеві простори імен для ізоляції контейнерів, запобігаючи прямому зв'язку між контейнерами, якщо це явно не налаштовано.

Використовуйте мережеві політики для контролю вхідного та вихідного трафіку між контейнерами та визначення правил взаємодії.

Постає питання, як керувати великою кількістю контейнерів з купою залежностей, адже управляти декількома контейнерами не складно, проте, якщо їх кількість постійно збільшується, як і буває в реальному світі, то треба впроваджувати системи оркестрації, такі як Kubernetes.

Необхідно ввести поняття Kubernetes. Kubernetes, часто скорочено K8s, – це платформа оркестрування контейнерів з відкритим вихідним кодом, призначена для автоматизації розгортання, масштабування та управління контейнерними додатками. Kubernetes забезпечує надійну і розширювану основу для розгортання і управління контейнерними додатками в масштабі.

У Kubernetes можливо захистити доступ до API за допомогою RBAC та впровадити контроль доступу на основі ролей для обмеження дозволів. Присутні вбудовані інструменти та зовнішні рішення для керування та безпечного розгортання конфіденційної інформації, наприклад, ключів API або паролів до баз даних.

Контейнери мають бути правильно налаштовані для створення журналів, і також має бути запроваджено централізоване рішення для збору для ведення журналів та регулярного їх перегляду на предмет подій безпеки.

Багаторівневий підхід до безпеки поєднує кілька заходів безпеки для створення більш надійного та стійкого захисту від потенційних загроз.

Інструменти оркестрування контейнерів, такі як Kubernetes, відіграють ключову роль в управлінні, розгортанні та масштабуванні контейнерних додатків. Хоча ці інструменти надають значні переваги з точки зору автоматизації та масштабованості, вони також створюють унікальні міркування та виклики для безпеки контейнерів. Нижче буде розглянуто, як інструменти оркестрування контейнерів впливають на безпеку контейнерів.

Оркестратори автоматизують розгортання і масштабування контейнерів, забезпечуючи узгоджену і передбачувану поведінку додатків. Автоматизовані

процеси можуть зменшити ймовірність помилок ручного налаштування, які можуть призвести до вразливостей у системі безпеки.

Автоматизований характер оркестрування може також посилити вплив неправильних конфігурацій, якщо ним не керувати належним чином. Найкращі практики безпеки слід інтегрувати в робочі процеси автоматизації, щоб зменшити ризики.

Інструменти оркестрування надають вбудовані засоби виявлення сервісів і балансування навантаження, спрощуючи управління мікросервісами. Це сприяє підвищенню доступності та відмовостійкості.

Динамічна природа контейнерних середовищ може призвести до збільшення поверхні атаки та потенційних вразливостей, якщо конфігурації виявлення сервісів та балансування навантаження не захищені належним чином.

Оркестратори часто пропонують вбудовані механізми для керування та розповсюдження секретів, таких як ключі API та паролі до баз даних. Це допомагає уникнути жорсткого кодування конфіденційної інформації у файлах конфігурації.

Ефективне керування секретами вимагає ретельної конфігурації, щоб забезпечити безпечну обробку та передачу конфіденційних даних. Витік або неправильне керування секретами може призвести до серйозних порушень безпеки.

Оркестратори дозволяють визначати мережеві політики та сегментацію, що дає змогу тонко контролювати взаємодію між контейнерами. Це допомагає запобігти несанкціонованому доступу між контейнерами.

Складні мережеві конфігурації можуть створювати проблеми з безпекою, наприклад, неправильна конфігурація може призвести до ненавмисного вразливого доступу до сервісів. Належна сегментація мережі та застосування політик мають вирішальне значення.

Оркестратори полегшують застосування конфігурацій безпеки на рівні виконання, таких як політики безпеки контейнерів і контролери допуску, що підвищує загальний рівень безпеки контейнерів.

Налаштування та керування засобами безпеки на рівні виконання може бути складним завданням. Забезпечення належного застосування та регулярного аудиту політик безпеки має важливе значення для безпечного середовища.

Оркестранти, зокрема Kubernetes, використовують cgroups для керування та ізоляції ресурсів, забезпечуючи справедливий розподіл ресурсів між контейнерами. Це запобігає зловживанню ресурсами та підвищує загальну стабільність системи.

Неправильні конфігурації розподілу або обмеження ресурсів можуть вплинути на продуктивність додатків або призвести до сценаріїв відмови в обслуговуванні. Необхідний регулярний моніторинг та коригування налаштувань ресурсів.

Інструменти оркестрування спрощують процес оновлення та відкату програм, дозволяючи швидко реагувати на вразливості безпеки. Це сприяє проактивній позиції безпеки.

Автоматизовані оновлення можуть спричинити проблеми сумісності або неочікувану поведінку. Ретельне тестування та перевірка мають вирішальне значення для забезпечення того, щоб оновлення не ставили під загрозу стабільність або безпеку середовища.

Оркестранти часто надають централізовані можливості ведення журналів та моніторингу, агрегуючи журнали та метрики з усього контейнерного середовища. Це полегшує виявлення інцидентів безпеки.

Налаштування ефективного ведення журналів і моніторингу вимагає ретельного планування того, що саме реєструвати і як інтерпретувати дані. Важливо визначити пороги оповіщення та регулярно переглядати журнали на предмет подій безпеки.

Оркестратори інтегруються з системами керування ідентичностями та доступом, що дає змогу визначати ролі та дозволи для користувачів і служб. Це допомагає забезпечити дотримання принципу найменших привілеїв.

Складність керування конфігураціями контролю доступу на основі ролей (RBAC) може призвести до неправильних конфігурацій, що потенційно може

призвести до вразливості конфіденційних ресурсів. Регулярні аудити та огляди є важливими для підтримання безпечного контролю доступу.

Оркестрування контейнерів сприяє розвитку концепції незмінної інфраструктури, де контейнери замінюються, а не оновлюються. Це зменшує ризик вразливостей під час виконання, що зберігаються у середовищі.

Впровадження незмінної інфраструктури вимагає надійних конвеєрів CI/CD та контролю версій. Забезпечення узгодженої збірки та розгортання образів має вирішальне значення для підтримки безпеки.

Інструменти оркестрування контейнерів суттєво впливають на безпеку контейнерів, автоматизуючи ключові аспекти управління контейнерами. Хоча ці інструменти пропонують численні переваги, організаціям важливо вирішувати пов'язані з ними проблеми і впроваджувати кращі практики безпеки в свої контейнерні робочі процеси. Регулярний аудит, моніторинг і проактивне управління ризиками мають вирішальне значення для підтримки безпечного середовища оркестрування контейнерів.

1.2 Огляд сторонніх засобів для підвищення безпеки контейнера

Для посилення безпеки контейнерів Docker доступні численні сторонні інструменти та рішення. Ці інструменти стосуються різних аспектів безпеки контейнерів, зокрема сканування зображень, захисту під час виконання, управління вразливостями тощо. Майте на увазі, що ефективність цих інструментів може відрізнятися в залежності від конкретних випадків використання і вимог організації. Нижче наведено огляд деяких популярних сторонніх інструментів, призначених для підвищення безпеки контейнерів Docker.

Clair - це сканер безпеки зображень контейнерів з відкритим вихідним кодом [7]. Він виявляє вразливості в образах контейнерів, інтегрується з реєстрами контейнерів для автоматичного сканування зображень. Основною перевагою є забезпечення видимості потенційних вразливостей перед розгортанням

контейнерів та підтримка інтеграцію з конвеєрами CI/CD для автоматичного сканування.

Anchore Engine - це інструмент для сканування образів і застосування політик з відкритим вихідним кодом. Основними функціями є сканування зображення контейнерів на наявність вразливостей і застосовує політики, що налаштовуються, підтримка аналіз зображень на предмет вмісту, метаданих і рівнів файлової системи.

Перевагами стануть інтегрування з робочими процесами CI/CD для безперервної перевірки безпеки, можливість перевіряти безпеку та відповідність вимогам на основі політик.

Aqua Security – це комплексна платформа для захисту контейнерів, що забезпечує захист під час виконання від атак і аномальної поведінки та впроваджує політики безпеки та засоби контролю під час виконання. Забезпечує сегментацію мережі, брандмауер і виявлення аномалій та підтримує криміналістику під час виконання та реагування на інциденти.

Sysdig Secure – це платформа для захисту та моніторингу контейнерів, яка забезпечує безпеку під час виконання з виявленням аномалій та скануванням вразливостей. Також забезпечує моніторинг цілісності файлів і сегментацію мережі. Інтегрується з платформами оркестрування для безперешкодного розгортання. Включає перевірку відповідності та аудиторські сліди.

K-Rail – це інструмент з відкритим вихідним кодом для впровадження політик безпеки у Kubernetes. Дозволяє визначати та застосовувати політики безпеки, та підтримувати перевірку політик у реальному часі та звітування.

Twistlock, який зараз є частиною хмарної платформи Palo Alto Networks Prisma Cloud, надає хмарну платформу безпеки. Забезпечує захист під час виконання, управління вразливостями та перевірку відповідності вимогам.

Для керування секретами можна використати HashiCorp Vault - рішення для керування секретами. Керує конфіденційною інформацією, такою як ключі API та паролі. Інтегрується з контейнерними середовищами для безпечного пошуку

секретів. Забезпечує безпечне зберігання та динамічний пошук секретів. Підтримує детальний контроль доступу та ведення журналів аудиту.

Cilium – це проект з відкритим вихідним кодом у сфері мережевих технологій та безпеки. Забезпечує мережеву безпеку, балансування навантаження та видимість мережі з підтримкою API. Забезпечує дотримання детальних мережевих політик для обміну контейнерами. Підвищує рівень мережевої безпеки завдяки таким функціям, як eBPF та IPsec. Забезпечує захист мікросервісів на основі ідентичностей.

Snyk - це платформа для сканування безпеки та вразливостей контейнерів з відкритим вихідним кодом. Сканує зображення контейнерів на наявність вразливостей. Пропонує сканування залежностей для контейнерних додатків. Надає дієві висновки та рекомендації щодо усунення вразливостей. Інтегрується з конвеєрами CI/CD і реєстрами контейнерів.

Ці сторонні інструменти сприяють комплексному підходу до безпеки контейнерів Docker, розглядаючи різні аспекти життєвого циклу контейнера. При виборі інструментів організації повинні враховувати свої конкретні вимоги до безпеки, можливості інтеграції з існуючими робочими процесами, а також рівень автоматизації та наочності, який вони пропонують. Регулярне оновлення та тестування цих інструментів має важливе значення для того, щоб випереджати нові загрози та вразливості в середовищі контейнерної безпеки, що швидко розвивається. Розробки у сфері безпеки контейнерів Docker продовжують розвиватися. Найбільш популярними поглядами на безпеку середовища контейнерів описані нижче [8].

Підхід "зсув вліво" передбачає інтеграцію заходів безпеки на більш ранніх етапах життєвого циклу розробки програмного забезпечення, що дозволяє розробникам виявляти і вирішувати проблеми безпеки на етапі кодування. Ця тенденція підкреслює важливість включення практик безпеки в конвеєр DevOps, включаючи контейнерні додатки, з самого початку.

З ростом використання контейнерів у виробничих середовищах зросла увага до безпеки під час виконання. Це включає моніторинг та захист контейнерів під час їх виконання. Інструменти та платформи, які пропонують функції безпеки під час виконання, такі як виявлення аномалій, аналіз поведінки та криміналістика під час виконання, набувають все більшого значення для виявлення та реагування на загрози в режимі реального часу.

Безпека всього ланцюжка постачання контейнерів, від розробки до розгортання, стала критично важливою. Це включає забезпечення безпеки образів контейнерів, залежностей і конвеєра CI/CD. Рішення, що забезпечують сканування зображень, оцінку вразливостей та безпечні практики CI/CD, необхідні для запобігання впровадженню вразливостей на будь-якому етапі ланцюга постачання.

Модель безпеки з нульовою довірою передбачає, що жодному об'єкту - як всередині, так і поза мережею - не слід довіряти за замовчуванням. Цей підхід все частіше застосовується до контейнерних середовищ. Впровадження нульової довіри передбачає перевірку та підтвердження всіх комунікацій, автентифікацію користувачів та служб, а також постійний моніторинг на предмет аномальної поведінки.

Концепція незмінної інфраструктури, коли контейнери замінюються, а не оновлюються, набуває все більшої популярності. Практики GitOps, які передбачають використання репозиторіїв з контролем версій для управління інфраструктурою, також сприяють підвищенню безпеки. Інфраструктура зменшує поверхню атаки, гарантуючи, що контейнери завжди розгортаються з відомого і безпечного стану. GitOps підвищує безпеку, увімкнувши декларативні конфігурації, що зберігаються у контролі версій.

Оскільки безсерверні обчислення набувають популярності, вони перетинаються з безпекою контейнерів. Це передбачає захист середовища виконання для безсерверних функцій, які можуть виконуватися у контейнерах. Міркування безпеки для безсерверних архітектур, такі як захист середовища

виконання функцій та керування контролем доступу, стають невід'ємною частиною загальних стратегій безпеки контейнерів.

Безпека контейнерів Docker продовжує розвиватися, щоб відповідати на виклики, пов'язані з витонченими кіберзагрозами і все більш широким впровадженням технологій контейнеризації. Організації застосовують комплексний підхід, інтегруючи заходи безпеки протягом усього життєвого циклу контейнера і використовуючи нові технології для поліпшення можливостей виявлення загроз і реагування на них. Будьте в курсі останніх подій у сфері безпеки контейнерів, щоб забезпечити надійну та адаптивну систему безпеки для ваших контейнерних додатків.

1.3 Постановка завдання

Дослідивши вразливості та способи захисту від них було визначено перелік завдань, які потрібно виконати для розробки системи аналізу середовища, де саме контейнер буде знаходитись:

- Запропонувати метод для підвищення безпеки Docker-контейнерів.
- Розробити підхід до сканування операційної системи всередині Docker на вразливості, які стосуються можливостей порушення віртуалізації.
- Розробити модуль для перевірки налаштувань Docker контейнерів та сповіщення користувача про неправильну конфігурацію.
- Скомпонувати розроблені, та існуючі рішення в цілісний продукт аналізу вразливості системи і рекомендації по їх усуненню.

Отже було розглянуто, що таке Docker та як відбувається віртуалізація контейнерів, вбудовані механізми для впровадження безпеки та рекомендації для їх конфігурації, такі як rootless доступ, та використання різних просторів імен під час запуску контейнерів. Розглянуто структуру Docker системи, та як відбувається

запуск і контроль контейнера. Проаналізовано існуючі вразливості Docker контейнерів та засобів віртуалізації в загальному.

Було розглянуто шляхи усунення вразливостей, таких як втеча з контейнера. Розглянуто існуючі системи сканування контейнерів на вразливості та проаналізовано їх сильні та слабкі сторони. Які бувають сторонні інструменти безпеки для docker-контейнерів, на які види вони поділяються та які краще застосовувати в тих чи інших умовах.

2 МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ DOCKER КОНТЕЙНЕРІВ

2.2Критерії оцінювання захищеності Docker контейнерів

Досить важко виділити якісь специфічні критерії оцінювання захищеності в якійсь певній величині, адже складно оцінити наскільки вдало захищені ті чи інші компоненти системи. На це впливає доцільність обраних критеріїв оцінювання саме для цього контейнеру. Найбільш вдалим критерієм може слугувати перелік одиниць захисту, які можна імплементувати і далі за цим рахувати скільки з цих захистів впроваджено та скільки ні. Тобто формула оцінки захищеності зводиться до наступної формули.

$$K = \frac{\text{КВКБ}}{\text{ЗККБ}}, \tag{2.1}$$

де K – коефіцієнт захищеності системи;

КВКБ – кількість впроваджених критеріїв безпеки;

ЗККБ – загальна кількість критеріїв безпеки.

Існує розроблений стандарт, який описує заходи безпеки, що мають бути імплементовані в середовищі віртуалізації. Один з найвідоміших стандартів є CIS Benchmark [9]. Існують різні варіанти цього файлу під різні операційні системи. В даній роботі фокус саме на версії CIS Benchmark for Ubuntu Linux 22.04 v1.0.0 від 30.08.2022. Назви критеріїв безпеки, що розподілені по секціям представлені у табл. 2.1.

Таблиця 2.1 – Секції та критерії безпеки CIS Benchmark for Ubuntu 22.04

Назва секції	Критерії безпеки
Конфігурація файлової системи	Ensure mounting of filesystems is disabled Ensure /tmp is a separate partition Ensure nodev, noexec, nosuid option set on /tmp partition Configure /var Ensure separate partition exists for /var Ensure nodev, nosuid option set on /var partition Protection of log data Ensure nodev, noexec, nosuid option set on /var/log partition Protection of user data Ensure nodev, nosuid option set on /home partition Configure /dev/shm Ensure nodev, noexec, nosuid option set on /dev/shm partition Ensure authentication required for single user mode

Продовження табл. 2.1

Конфігурація безпекових сервісів	Configure AppArmor Ensure AppArmor is enabled in the bootloader configuration . Ensure all AppArmor Profiles are in enforce or complain mode Services Configure Time Synchronization Special Purpose Services Ensure X Window System is not installed Ensure Avahi Server is not installed Ensure CUPS is not installed Ensure DHCP Server is not installed Ensure LDAP server is not installed Ensure NFS is not installed Ensure DNS Server is not installed Ensure FTP Server is not installed Ensure HTTP server is not installed Ensure IMAP and POP3 server are not installed Ensure Samba is not installed Ensure HTTP Proxy Server is not installed Ensure SNMP Server is not installed Ensure NIS Server is not installed Ensure mail transfer agent is configured for local-only mode Ensure rsync service is either not installed or masked Service Clients Ensure NIS Client is not installed Ensure rsh client is not installed Ensure talk client is not installed Ensure telnet client is not installed Ensure LDAP client is not installed Ensure RPC is not installed Ensure nonessential services are removed or masked (Manual)
Конфігурація мережевих налаштувань	Network Configuration Disable unused network protocols and devices Ensure system is checked to determine if IPv6 is enabled (Manual) Ensure wireless interfaces are disabled Network Parameters (Host Only) Ensure packet redirect sending is disabled Ensure IP forwarding is disabled Network Parameters (Host and Router). Ensure source routed packets are not accepted Ensure ICMP redirects are not accepted Ensure secure ICMP redirects are not accepted Ensure suspicious packets are logged Ensure broadcast ICMP requests are ignored Ensure bogus ICMP responses are ignored Ensure Reverse Path Filtering is enabled Ensure TCP SYN Cookies is enabled Ensure IPv6 router advertisements are not accepted
Конфігурація брандмауеру	Firewall Configuration Configure UncomplicatedFirewall

Продовження табл. 2.1

Конфігурація логування та аудиту	Logging and Auditing Configure System Accounting (auditd) Normalization Capacity planning Ensure auditing is enabled Configure Data Retention Configure auditd rules Ensure actions as another user are always logged Ensure events that modify the sudo log file are collected Ensure events that modify the system's network environment are collected Ensure use of privileged commands are collected Ensure unsuccessful file access attempts are collected Ensure events that modify user/group information are collected Ensure discretionary access control permission modification events are collected Ensure successful file system mounts are collected Ensure session initiation information is collected Ensure login and logout events are collected Ensure file deletion events by users are collected Ensure events that modify the system's Mandatory Access Controls are collected Ensure successful and unsuccessful attempts to use the chcon command are recorded Ensure successful and unsuccessful attempts to use the setfacl command are recorded Ensure successful and unsuccessful attempts to use the chacl command are recorded Ensure successful and unsuccessful attempts to use the usermod command are recorded Ensure kernel module loading unloading and modification is collected Ensure the audit configuration is immutable Ensure the running and on disk configuration is the same (Manual) Configure auditd file access Configure Logging Security principals for logging Configure journald Access, Authentication and Authorization Configure time-based job schedulers Ensure cron daemon is enabled and running Ensure permissions on /etc/crontab are configured Ensure permissions on /etc/cron.hourly are configured Ensure permissions on /etc/cron.daily are configured Ensure permissions on /etc/cron.weekly are configured Ensure permissions on /etc/cron.monthly are configured Ensure permissions on /etc/cron.d are configured Ensure cron is restricted to authorized users Ensure at is restricted to authorized users

Продовження табл. 2.1

Конфігурація підвищення привілеїв	Configure privilege escalation Ensure sudo is installed Ensure sudo commands use pty Ensure sudo log file exists Ensure users must provide password for privilege escalation Ensure re-authentication for privilege escalation is not disabled globally Ensure sudo authentication timeout is configured correctly . Ensure access to the su command is restricted
Конфігурація PAM модулів	Configure PAM User Accounts and Environment Ensure system accounts are secured Ensure default group for the root account is GID 0 Ensure default user umask is 027 or more restrictive Ensure default user shell timeout is 900 seconds or less
Конфігурація підтримки системи	System Maintenance
Конфігурація дозволів файлової системи	System File Permissions Ensure permissions on /etc/passwd are configured Ensure permissions on /etc/group are configured Ensure permissions on /etc/shadow are configured Ensure permissions on /etc/gshadow are configured Ensure no world writable files exist Ensure no unowned files or directories exist Ensure no ungrouped files or directories exist Audit SUID executables (Manual) Audit SGID executables (Manual) Local User and Group Settings Ensure accounts in /etc/passwd use shadowed passwords Ensure /etc/shadow password fields are not empty Ensure all groups in /etc/passwd exist in /etc/group Ensure shadow group is empty Ensure no duplicate UIDs exist Ensure no duplicate GIDs exist Ensure no duplicate user names exist Ensure no duplicate group names exist Ensure root PATH Integrity Ensure root is the only UID 0 account Ensure local interactive user home directories exist Ensure local interactive users own their home directories Ensure local interactive user home directories are mode 750 or more restrictive

Усі ці критерії безпеки необхідно впроваджувати у Docker-контейнерах, але зазвичай адміністратори систем сподіваються на ізольованість середовища контейнеризації, і тому нехтують налаштуваннями всередині контейнеру. Але це

не так. Шкідливе програмне забезпечення може потрапити в контейнер зовсім неочікувано, і до цього треба бути готовим.

2.3 Практичне дослідження методу сканування і виправлення конфігурацій

Trivy – це сканер вразливостей з відкритим вихідним кодом, розроблений для контейнерних середовищ [10]. Його основне призначення – виявляти проблеми безпеки в образах контейнерів і файлових системах. Цей інструмент зазвичай використовується в конвеєрах DevOps і платформах оркестрування контейнерів, таких як Kubernetes.

Trivy пропонує кілька ключових функцій, включаючи можливість сканувати образи контейнерів на наявність вразливостей в програмних пакетах і бібліотеках. Він також аналізує файлову систему контейнерів для виявлення проблем безпеки, досліджуючи як встановлене програмне забезпечення, так і конфігурації.

Інструмент інтегрується з базами даних безпеки, використовуючи інформацію з таких джерел, як National Vulnerability Database (NVD), для виявлення відомих вразливостей, пов'язаних з версіями використовуваних програмних компонентів.

Trivy відомий своїми можливостями автоматизації та інтеграції, що дозволяє легко інтегрувати його в конвеєри CI/CD та робочі процеси оркестрування контейнерів. Це гарантує, що образи контейнерів автоматично скануються на наявність вразливостей в рамках процесів розробки та розгортання.

Швидкий і легкий, Trivy добре підходить для швидкого реагування на проблеми безпеки. Він підтримує декілька менеджерів пакетів, включаючи APT, Yum, Apk та інші, що робить його універсальним і сумісним з різними дистрибутивами Linux і системами управління пакетами.

Загалом, Trivy сприяє підвищенню рівня безпеки контейнерних середовищ, полегшуючи раннє виявлення та усунення вразливостей у життєвому циклі

розробки програмного забезпечення. Його використання сприяє більш безпечному та надійному розгортанню контейнерних програм.

Однак використання Trivy не гарантує того, що ваш контейнер буде достатньо захищеним, адже він всього лиш повідомляє про наявність певних вразливостей та не виправляє їх. Ця задача дістається адміністраторам контейнеризованого середовища.

Давайте перевіримо, які вразливості Trivy зможе відшукати в образі контейнеру Ubuntu 20.04.

Для цього нам необхідно встановити Trivy. Для користувачів Mac все досить просто, всього на всього треба запустити команду

```
-> brew install trivy
Warning: trivy 0.48.0 is already installed and up-to-date.
```

Використання даного сканеру вразливостей досить просте. Необхідно вказати який образ сканувати, а решту він зробить сам.

```
(base) ➜  diploma trivy image ubuntu:20.04
2023-12-09T10:24:03.901+0200    INFO    Vulnerability scanning is enabled
2023-12-09T10:24:03.901+0200    INFO    Secret scanning is enabled
2023-12-09T10:24:03.901+0200    INFO    If your scanning is slow, please try '--
scanners vuln' to disable secret scanning
2023-12-09T10:24:03.933+0200    INFO    Detected OS: ubuntu
2023-12-09T10:24:03.933+0200    INFO    Detecting Ubuntu vulnerabilities...
2023-12-09T10:24:03.942+0200    INFO    Number of language-specific files: 0

ubuntu:20.04 (ubuntu 20.04)
Total: 17 (UNKNOWN: 0, LOW: 15, MEDIUM: 2, HIGH: 0, CRITICAL: 0)
```

З лістингу вище видно скорочено версію виводу даної утиліти, яка містить системну інформацію. Нижче на рис. 2.1. детально описано, які були знайдені вразливості, їх важливість, який файл або бібліотека є вразливою, а також посилання на CVE сайт, для більш детального ознайомлення з вибраною вразливістю.

Наприклад утиліта tar: (CVE-2023-39804): Уразливість переповнення стеку середньої важкості в GNU Tar до версії 1.34 включно.

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2		coreutils: Non-privileged session can escape to the parent session in chroot https://avd.aquasec.com/nvd/cve-2016-2781
gpgv	CVE-2022-3219			2.2.19-3ubuntu2.2		denial of service issue (resource consumption) using compressed packets https://avd.aquasec.com/nvd/cve-2022-3219
libc-bin	CVE-2016-20013			2.31-0ubuntu9.12		sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of... https://avd.aquasec.com/nvd/cve-2016-20013
	CVE-2023-4806		fixed		2.31-0ubuntu9.14	glibc: potential use-after-free in getaddrinfo() https://avd.aquasec.com/nvd/cve-2023-4806
	CVE-2023-4813					glibc: potential use-after-free in gaih_inet() https://avd.aquasec.com/nvd/cve-2023-4813
libc6	CVE-2016-20013		affected			sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of... https://avd.aquasec.com/nvd/cve-2016-20013
	CVE-2023-4806		fixed		2.31-0ubuntu9.14	glibc: potential use-after-free in getaddrinfo() https://avd.aquasec.com/nvd/cve-2023-4806
	CVE-2023-4813					glibc: potential use-after-free in gaih_inet() https://avd.aquasec.com/nvd/cve-2023-4813
liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1		Denial of service via decompression of crafted file https://avd.aquasec.com/nvd/cve-2020-22916
libpcre3	CVE-2017-11164	LOW		2:8.39-12ubuntu0.1		OP_KETRMAX feature in the match function in pcre_exec.c https://avd.aquasec.com/nvd/cve-2017-11164
libsystemd0	CVE-2023-26604			245.4-4ubuntu3.22		systemd: privilege escalation via the less pager https://avd.aquasec.com/nvd/cve-2023-26604
libudev1						
login	CVE-2013-4235			1:4.8.1-1ubuntu5.20.04.4		shadow-utils: TOCTOU race conditions by copying and removing directory trees https://avd.aquasec.com/nvd/cve-2013-4235
	CVE-2023-29383					Improper input validation in shadow-utils package utility chfn https://avd.aquasec.com/nvd/cve-2023-29383
passwd	CVE-2013-4235					shadow-utils: TOCTOU race conditions by copying and removing directory trees https://avd.aquasec.com/nvd/cve-2013-4235
	CVE-2023-29383					Improper input validation in shadow-utils package utility chfn https://avd.aquasec.com/nvd/cve-2023-29383
tar	CVE-2023-39804	MEDIUM		1.30+dfsg-7ubuntu0.20.04.3		[A stack overflow vulnerability exists in GNU Tar up to including v1.34.... https://avd.aquasec.com/nvd/cve-2023-39804

Рисунок 2.1 – Результат сканування образа Ubuntu утилітою Trivy

Вкрай важливо усунути цю вразливість шляхом оновлення до їхніх виправлених версій або застосуванням відповідних патчів. Регулярний моніторинг та оновлення програмних компонентів є важливими практиками для підтримки безпечної системи. Ця задача може бути виконана за допомогою Ansible та використанням методу, що буде описаний пізніше [11].

2.4 Розробка методу підвищення захищеності Docker-контейнерів

Групою користувачів було створено ansible-playbook, що дозволяє аналізувати і виправляти перелічені в попередньому підрозділі критерії безпеки для віддалених машин.

Необхідно розглянути як дане рішення працює, та які критерії перевірки в ньому присутні, для цього нам необхідно скачати з github.com репозиторій під назвою alivx/CIS-Ubuntu-20.04-Ansible та переглянути його вміст [12]. Всередині ми можемо бачити наступну структуру директорії, як на рис. 2.2.

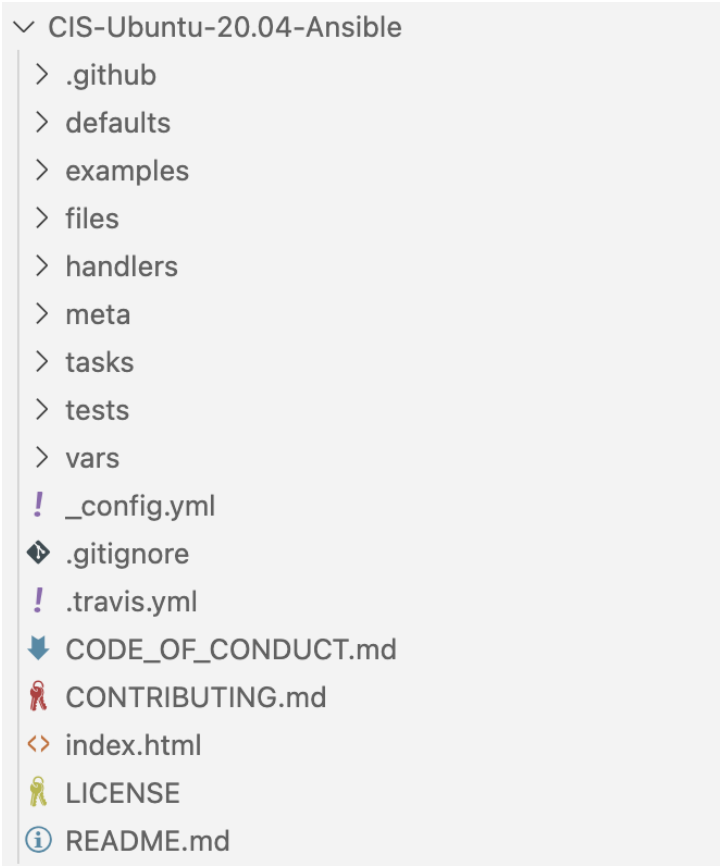


Рисунок 2.2 – Структура репозиторію alivx/CIS-Ubuntu-20.04-Ansible

Головна частина описана у директорії tasks, що описує усі представлені перевірки з файлу CIS Ubuntu 20.04 Benchmark. Як можна бачити з рис 2.3 для кожної секції є свій набір правил, описаний від початку до кінця. Можна перевіряти як і кожну секцію окремо, так і всі разом. Якщо необхідно включити або відключити деякі перевірки, їх можна знайти саме в цих файлах, та видалити або закоментувати, після чого використовувати вже виправлений варіант.

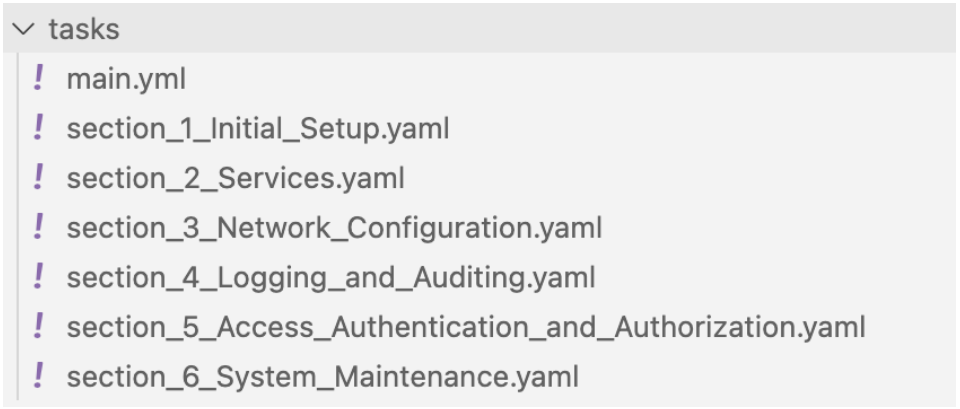


Рисунок 2.3 – Структура директорії CIS-Ubuntu-20.04-Ansible/tasks

Розглянемо, що знаходиться у файлі section4_Logging_and_Auditing.yaml. Нижче наведена частина цього файлу. Повний файл можна переглянути у додатку Г.

```
# 4.1.2.1 Ensure audit log storage size is configured
- name: 4.1.2.1 Ensure audit log storage size is configured
 lineinfile:
   dest: /etc/audit/auditd.conf
   regexp: "^max_log_file( |=)"
   line: "max_log_file = {{ max_log_file }}"
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.2.1
# 4.1.2.2 Ensure audit logs are not automatically deleted
- name: 4.1.2.2 Ensure audit logs are not automatically deleted
 lineinfile:
   dest: /etc/audit/auditd.conf
   regexp: "^max_log_file_action"
   line: "max_log_file_action = {{ max_log_file_action }}"
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.2.2
```

З частини цієї YAML конфігурації ми можемо побачити дві перевірки, що здійснюються під час сканування:

– перевірка чи зконфігуровано розмір файлів для логування;

– чи видаляються автоматично лог файли.

Приклади роботи цього рішення будуть наведені далі. Для перевірки було створено віртуальну машину у хмарі AWS Ubuntu 20.04. Ось як це виглядає у Amazon Web Console рис. 2.4.

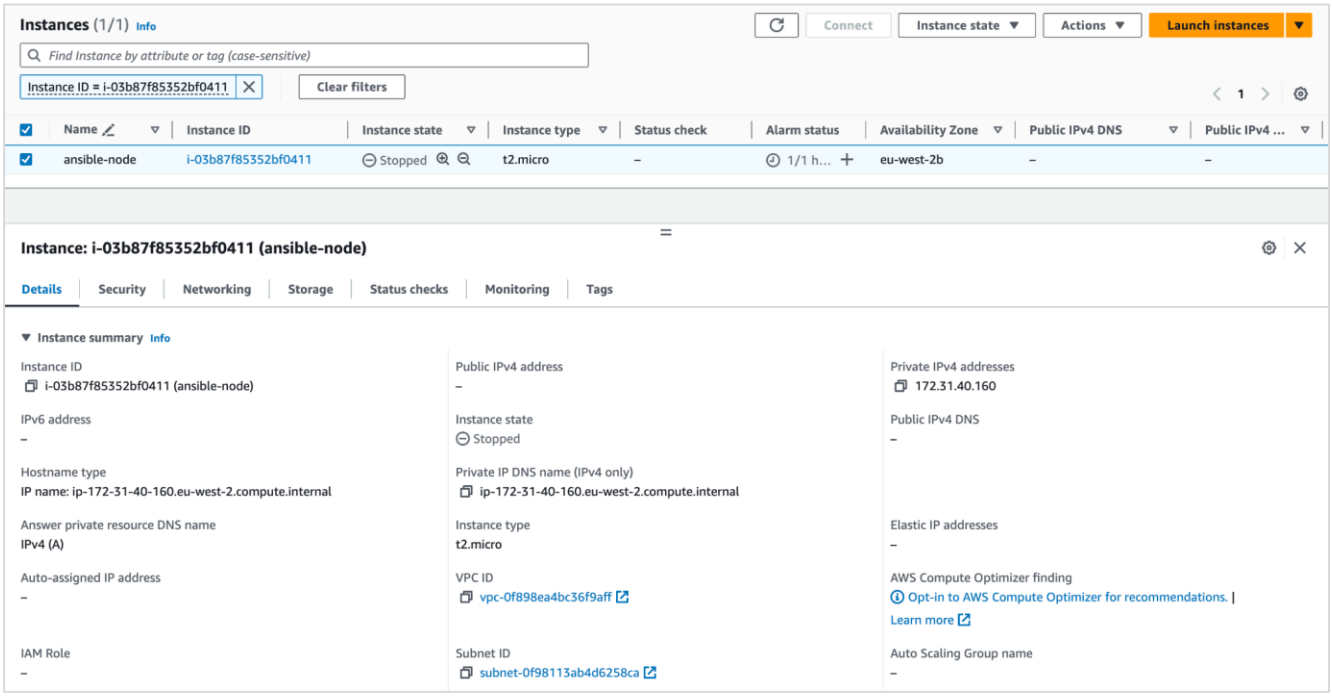


Рисунок 2.4 – Amazon Web Console з тестовою віртуальною машиною

Зконфігуровано SSH ключі певним чином, щоб був безпарольний доступ до віртуальної машини. Вказані правильні налаштування для використання ansible-playbook, а саме ім’я віддаленого користувача та IP адреса віртуальної машини. Конфігурація складається з двох файлів: host та run.yaml зображених на рис. 2.5 та рис. 2.6.

```
1   [host1]
2   54.224.177.250
```

Рисунок 2.5 – Файл host

Файл host в собі містить перелік всіх хостів, що будуть просканові. Також в цьому файлі можна окремо вказати користувача від імені якого буде відбуватися автентифікація на віддаленій машині.

Після того, як всі файли кладені в одне місце, а репозиторій з необхідними конфігураціями склонований з GitHub, можна розпочинати тестування.

```yaml
---
- hosts: host1
  # connection: local
  become: yes
  remote_user: ubuntu
  gather_facts: no
  roles:
      - { role: "CIS-Ubuntu-20.04-Ansible" }
```

Рисунок 2.6 – Файл run.yaml

Вигляд робочої директорії перед виконанням команди для сканування та виправлення помилок (рис. 2.7).

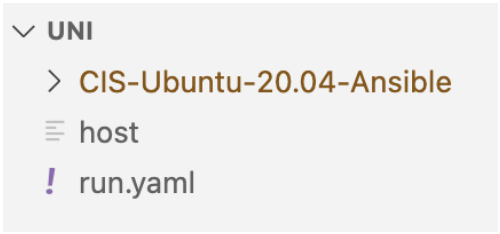


Рисунок 2.7– Структура директорії перед запуском команди

Команда, яка запускає ansible-playbook та розпочинає сканування з виправленням конфігурації віддаленого хоста, відповідно до описаних конфігураційних файлів у директорії CIS-Ubuntu-20.04-Ansible представлена нижче.

```
ansible-playbook -i host run.yaml -v -t section3
```

В конкретно цьому прикладі ми скануємо тільки те, що стосується третьої секції документу CIS Benchmark. Повний вивід представлено в додатку В.

```
(base) ➜  Uni ansible-playbook -i host run.yaml -v -t section3
No config file found; using defaults
TASK [CIS-Ubuntu-20.04-Ansible : 3.1.1 Disable IPv6] ***************************************
ok: [54.224.177.250] => {"ansible_facts": {"discovered_interpreter_python":
"/usr/bin/python3"}, "changed": false, "msg": "", "rc": 0}

TASK [CIS-Ubuntu-20.04-Ansible : verify no wireless interfaces are active on the system]
**
changed: [54.224.177.250] => {"changed": true, "rc": 0, "stderr": "Shared connection to
54.224.177.250 closed.\r\n", "stderr_lines": ["Shared connection to 54.224.177.250
closed."], "stdout": "Wireless is not enabled\r\n", "stdout_lines": ["Wireless is not
enabled"]}
```

```
TASK [CIS-Ubuntu-20.04-Ansible : 3.1.2 Ensure wireless interfaces are disabled]
***********
skipping: [54.224.177.250] => {"changed": false, "false_condition":
"wifiStatus.stdout_lines ==  \"Wireless is not enabled\"", "skip_reason": "Conditional
result was False"}

******************
SKIPPING OUTPUT
******************
PLAY RECAP *********************************************************************
54.224.177.250: ok=49 changed=44 unreachable=0 failed=0    skipped=3    rescued=0
ignored=0
```

З прикладу видно, як почалось сканування системи від імені користувача ubuntu на віддаленому хості з IP адресою 54.224.177.250. Було виконано три завдання: відключення IPv6, перевірка бездротових підключень та наявність бездротового інтерфейсу. Велика частину виводу програми була пропущена через велику кількість даних, проте система відпрацювала гарно.

Всього було виконано 49+44+3 перевірки. Але перед тим як продовжити необхідно визначити, що значить кожен зі статусів перевірки.

- Ok – Кількість завдань, які були успішно виконані без проблем.
- Changed – Кількість завдань, які спричинили зміни в системі. Це може означати, що щось було змінено або оновлено.
- Unreachable – Кількість хостів, з якими Ansible не зміг зв'язатися. Це може бути пов'язано з мережевими проблемами, неправильними обліковими даними або несправністю хоста.
- Failed – Кількість завдань, які зіткнулися з помилками або не змогли виконатися належним чином.
- Skipped – Кількість завдань, які було пропущено під час виконання. Це може статися, якщо умову завдання не було виконано або якщо його було явно пропущено.
- Rescued – Кількість завдань, які було врятовано блоком, що перехоплює помилки. Це важливо, якщо ви використовуєте рятувальне речення у завданнях Ansible.

- Ignored – Кількість завдань, які було проігноровано. Це може статися при використанні параметра ignore_errors або подібних механізмів, які дозволяють продовжити виконання сценарію, незважаючи на помилки.

Просканована систему можна оцінити за запропонованою раніше формулою (2.1) підставивши в неї відповідні значення.

$$\frac{49+44}{49+44+3} = \frac{93}{96} = 0.96$$

Отже наша система відповідно до секції 3 відповідає вимогам аудиту на 96%. Це є дуже високим рівнем захищеності, проте це тільки одна секція, щоб довести, що система має захист від різних векторів атак треба перевірити також і інші секції документа CIS.

Використаний метод можна представити за допомогою рис. 2.8.

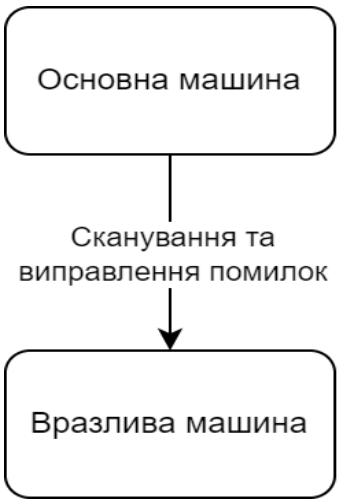


Рисунок 2.8 – Діаграма розташування хостів при проведенні скануванні

На рисунку зображено, що віддалена машина під’єднується до вразливої машини, щоб виконати сканування та виправлення помилок конфігурації. Слід зауважити, що це не одна і та сама машина, і сканування відбувається з іншого хоста.

Наразі відсутнє рішення, яке оцінювало б Docker-контейнери з системи хоста без вказання IP адрес, відкриття SSH портів, підкладання сертифікатів і створення

повноцінного звіту. Також відсутні інструменти для оцінки найновішої системи Ubuntu 22.04 з новими критеріями захисту.

Пропонується покращити існуюче рішення для сканування віртуальних машин та створити його модуль для аналізу та оцінки docker контейнерів на базі операційної системи Ubuntu, що вирішить задачу складної конфігурації контейнерів, зменшить кількість ручної роботи, створюватиме документ з оцінкою кожного окремого контейнера, хоста, та навіть групи хостів.

Новий метод для підвищення безпеки у Docker контейнерах може бути представлений такими кроками:

1) Виявлення Docker контейнера.
2) Збір інформації про Docker контейнер.
3) Створення Docker SSH сервер контейнеру для підключення.
4) Підключення до необхідного Docker контейнеру.
5) Аналіз Docker контейнера за критеріями CIS Ubuntu Linux 20.04 Benchmark.
6) Виправлення конфігурацій, що не відповідають критеріям:
   - вимкнути програми, що не використовуються;
   - зміна конфігурації мережі;
   - відключити пристрої та мережеві протоколи, що не використовуються.
7) Надсилаємо звіт адміністратору системи.

Даний метод можна реалізувати за допомогою різних мов програмування. Проте при виконанні даної роботи було вирішено використовувати наступні інструменти:

- Ansible – інструмент для сканування та виправлення конфігурації.
- Bash скрипт – набір команд командної оболонки, що збиратимуть метадані про контейнери, запускатимуть Ansible та розгортатимуть docker ssh server.
- Docker + Docker SSH Server.

Якщо представити даний момент у вигляді алгоритму, то буде отримано наступну схему, що зображено на рис. 2.9.

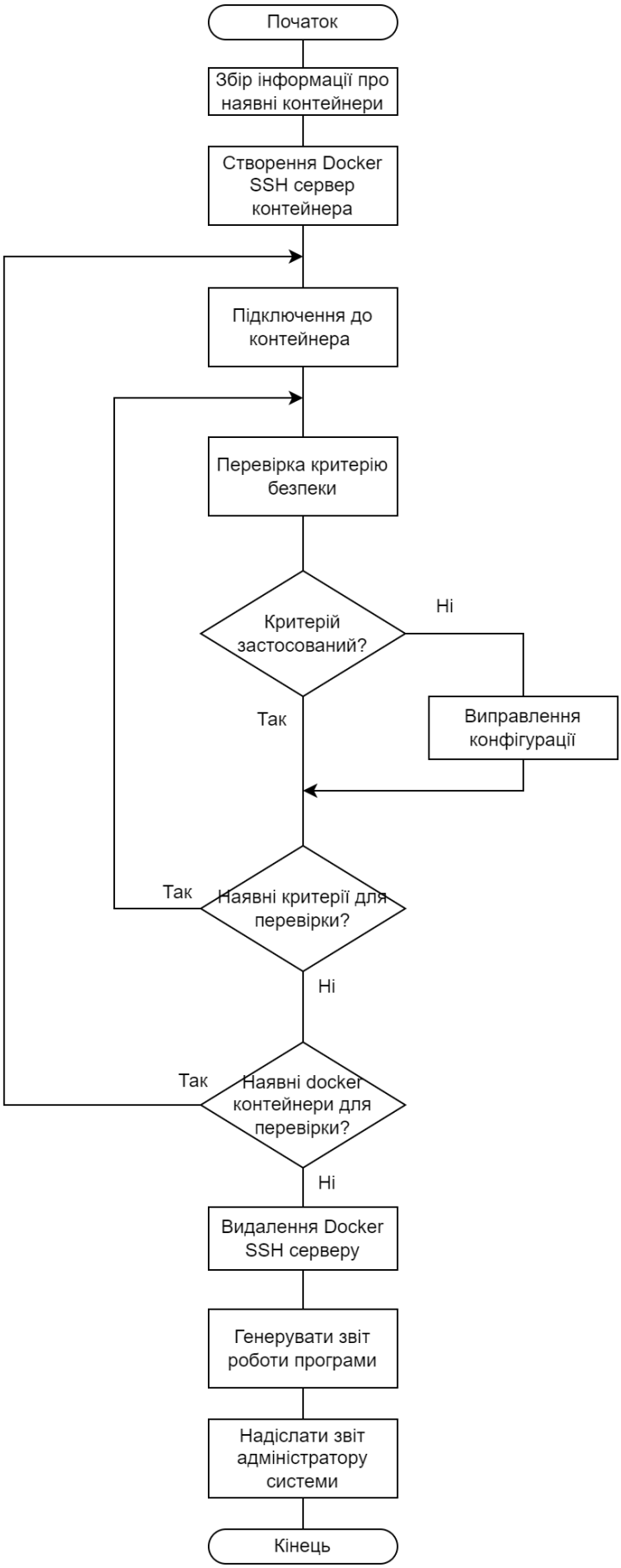


Рисунок 2.9 – Алгоритм роботи методу

Перед початком розробки треба визначитися з інструментами, які будуть використовуватися для тих чи інших задач в залежності від потреби. З представленого алгоритму кожен крок використовує певні технології, які треба заздалегідь визначити, тож список наведено нижче.

1) Збір інформації про наявні контейнери – збір відбуватиметься за допомогою docker inspect утиліти, яка дозволяє дізнатись дані про про контейнер, такі як: коли був запущений, яку адресу має, яке ім’я і таке інше.
2) Створення Docker SSH сервера – за допомогою docker run ми маємо створити контейнер, який дозволить в майбутньому підключатися до вибраного контейнера з тим способом автентифікації, який нам потрібно [13]. Наприклад метод з відсутністю автентифікації нам цілком підходить, адже даний docker ssh server буде видалено після завершення тестування, тож це підвищує ризик на короткий час.
3) Підключення до контейнера – підключення до контейнера відбувається під час використання Ansible Playbook. Ansible підключається до вказаного контейнера, в даному випадку це Docker SSH Server, який переправляє з’єднання до потрібного нам контейнера.
4) Перевірка критерію безпеки – критерії безпеки описані в директорії CIS-Ubuntu-20.04-Ansible/tasks. Критерії безпеки вже були згадані у попередньому розділі. Увімкнення чи вимкнення тих чи інших перевірок відбувається у файлі CIS-Ubuntu-20.04-Ansible/defaults/main.yml
5) Перевірка, чи критерій застосований, якщо так, то перевірити чи ще присутні критерії для перевірки. Якщо присутні, продовжити перевірку, якщо ж ні, то закінчити роботу над вказаним контейнером. Якщо критерій не застосований, то виправити його та перевірити, чи ще присутні критерії безпеки для перевірки.
6) Якщо з контейнером закінчено, то взяти наступний, або якщо це був останній, то видалити SSH Docker Server.
7) Згенерувати звіт та відправити адміністратору.

3 РОЗРОБКА ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ПРОГРАМНОГО ЗАСТОСУНКУ

Для початку розробки програмного додатку для методу підвищення захисту Docker-контейнерів встановимо інтерпретатор python, адже він потрібний для Ansible. Для цього необхідно перейти на офіційний сайт python (рис. 3.1) та завантажити його для операційної системи встановленої на комп'ютері [14].

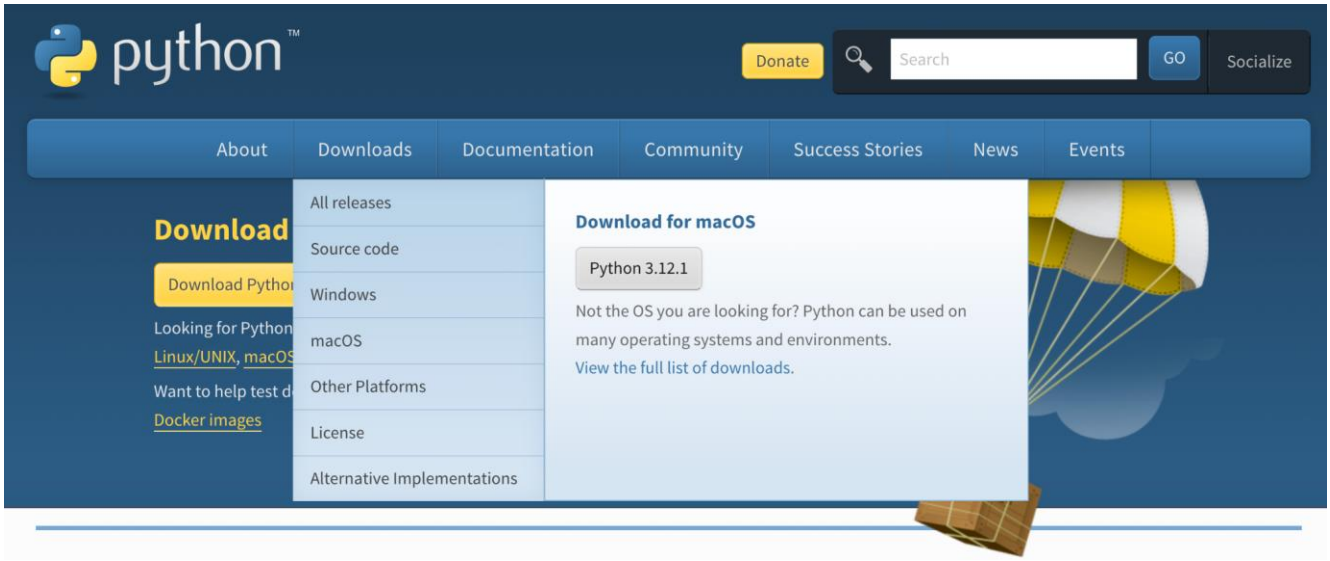


Рисунок 3.1 – Офіційний сайт Python

Це не єдиний спосіб для встановлення python, користувач може сам обрати зручний йому спосіб. Наприклад через такі пакетні менеджери як apt, yum, pacman, brew, тощо.

Перевірити чи успішно його встановлено можна за допомогою терміналу встановленого на вашому комп'ютері. Достатньо набрати команду як показано на рис. 3.2.

```
(base) ➜  Projects python --version
Python 3.11.5
```

Рисунок 3.2 – Команда для перевірки версії Python

Необхідна версія python хоча б 3.8 або вища. Наступним кроком йде встановлення ansible за допомогою python. Необхідно відмітити, що необхідна версія ansible 5.1.0. Адже деякі компоненти використовуваного ansible-playbook вже встигли застаріти, але вони знаходяться в процесі оновлення автором. Команда для встановлення ansible продемонстрована на рисунку 3.3.

```
(base) ➜  Projects python -m pip install ansible==5.1.0
Requirement already satisfied: ansible==5.1.0 in /Users/viacheslav.kozachok/miniconda3/lib/python3.11/site-packages (5.1.0)
Requirement already satisfied: ansible-core~=2.12.1 in /Users/viacheslav.kozachok/miniconda3/lib/python3.11/site-packages (
from ansible==5.1.0) (2.12.10)
Requirement already satisfied: jinja2 in /Users/viacheslav.kozachok/miniconda3/lib/python3.11/site-packages (from ansible-c
ore~=2.12.1->ansible==5.1.0) (3.1.2)
Requirement already satisfied: PyYAML in /Users/viacheslav.kozachok/miniconda3/lib/python3.11/site-packages (from ansible-c
ore~=2.12.1->ansible==5.1.0) (6.0.1)
Requirement already satisfied: cryptography in /Users/viacheslav.kozachok/miniconda3/lib/python3.11/site-packages (from ans
ible-core~=2.12.1->ansible==5.1.0) (41.0.3)
Requirement already satisfied: packaging in /Users/viacheslav.kozachok/miniconda3/lib/python3.11/site-packages (from ansibl
e-core~=2.12.1->ansible==5.1.0) (23.1)
Requirement already satisfied: resolvelib<0.6.0,>=0.5.3 in /Users/viacheslav.kozachok/miniconda3/lib/python3.11/site-packag
es (from ansible-core~=2.12.1->ansible==5.1.0) (0.5.4)
Requirement already satisfied: cffi>=1.12 in /Users/viacheslav.kozachok/miniconda3/lib/python3.11/site-packages (from crypt
ography->ansible-core~=2.12.1->ansible==5.1.0) (1.15.1)
Requirement already satisfied: MarkupSafe>=2.0 in /Users/viacheslav.kozachok/miniconda3/lib/python3.11/site-packages (from
jinja2->ansible-core~=2.12.1->ansible==5.1.0) (2.1.3)
Requirement already satisfied: pycparser in /Users/viacheslav.kozachok/miniconda3/lib/python3.11/site-packages (from cffi>=
1.12->cryptography->ansible-core~=2.12.1->ansible==5.1.0) (2.21)
(base) ➜  Projects
```

Рисунок 3.3 – Встановлення ansible конкретної вверсії

Також треба підготувати репозиторій з критеріями безпеки, які буде впроваджено у вразливі Docker-контейнери. Для цього необхідно склонувати репозиторій за допомогою git або завантажити його як архів, з github і розпакувати в робочій директорії

3.1 Розробка програмного додатку з використанням bash

Для розробки запропонованого методу використовуватимуться такі технології як Docker, Ansible та протокол захищенної комунікації SSH.

Також необхідно створити контейнери, з якими наша программа буде працювати. Для цього пропонується використати docker-compose-ubuntus.yaml файл, який створить нам три Ubuntu Server 20.04, що будуть піддослідними під час виконання нашої роботи. Саме на них буде тестуватися виконання програми, яка буде створена.

Приклад docker-compose-ubuntus.yaml файлу:

```
version: '3'

 ubuntu-web:
   image: ubuntu:20.04
   entrypoint: sleep infinity
   networks:
     - web

 ubuntu-db:
   image: ubuntu:20.04
   entrypoint: sleep infinity
   networks:
     - web

 ubuntu-proxy:
   image: ubuntu-local-proxy
   build: ./ubuntu-proxy/
   entrypoint: sleep infinity
   networks:
     - web

networks:
 web:
```

Результат виконання файлу представлений нижче. Варто зазначити, що дані контейнери створені з іменами по типу ubuntu-db, ubuntu-web та ubuntu-proxy для того, щоб імітувати набір контейнерів, який справді може зустрітися у мережі певної компанії, як зображено на рисунку 3.4. Також на них буде додатково встановлено відповідні компоненти. У якості веб сервера буде встановлено nginx, у якості бази даних PostgreSQL, у вигляді проксі Traefik.

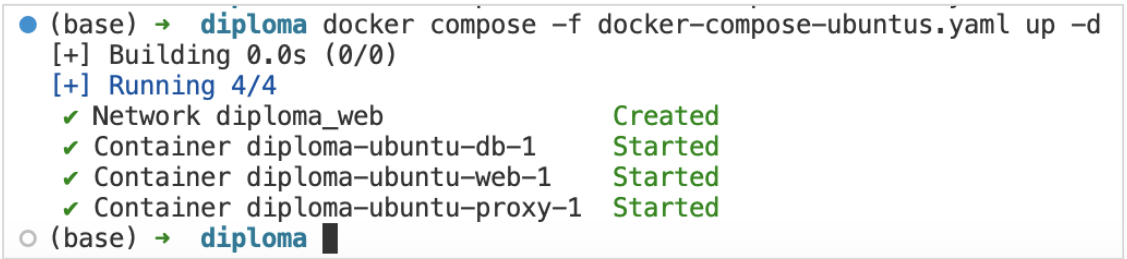


Рисунок 3.4 – Результат виконання команди docker compose up -d

Після вдалого запуску контейнерів необхідно необхідно зібрати інформацію про ці контейнери, таку як IP адреси, щоб виконати сканування контейнерів.

Створено таку команду, щоб створити список IP адрес

```
(base) ➜  diploma docker ps -q | xargs -n 1 docker inspect \
    --format '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' \
```

```
    | sed 's#^/##'
172.20.0.2
172.20.0.4
172.20.0.3
```

Як показано на рисунку 3.5, запущено 3 контейнери з попереднього кроку. Через графічний інтерфейс можемо впевнитись, що все відпрацювало коректно.

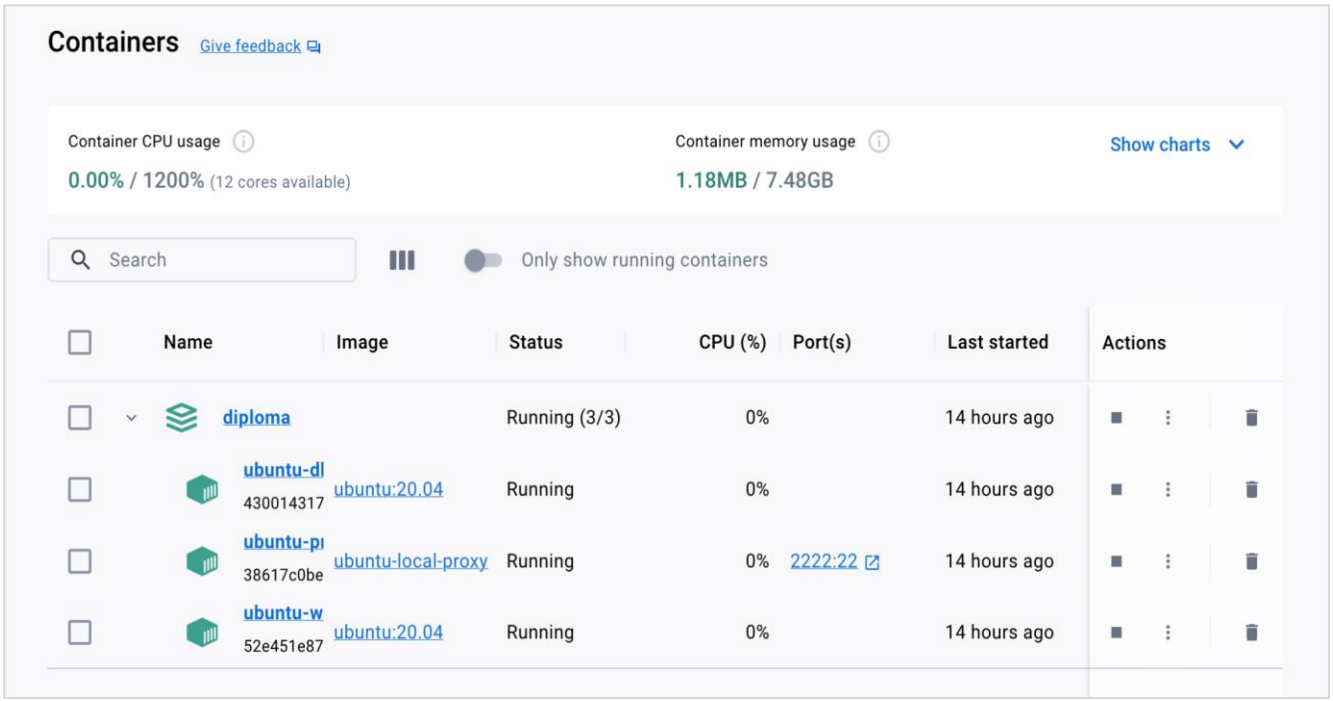


Рисунок 3.5 – Вигляд запущених Docker-контейнерів через графічний інтерфейс

На даному етапі можна приступити до розробки програмного коду. За наведеним алгоритмом у попередньому розділі було розроблено програму, код якої представлено у додатку Б.

Цей скрипт є сценарієм Ansible, призначеним для виконання сканування безпеки контейнерів Docker за допомогою тестів CIS (Center for Internet Security) для Ubuntu 20.04.

Першим кроком є встановлення змінних оточення, таких як `SCAN_DIR`, що вказує каталог `container-ansible-scan`, в якому буде виконано сканування Ansible. Наступна зміна, це `ANSIBLE_CONFIGURATION`, що містить конфігурацію

плейбука Ansible у форматі YAML. Вона визначає плейбук з назвою "CIS", націлений на хости з іменами "myhosts" з певними ролями, зокрема "CIS-Ubuntu-20.04-Ansible".

Наступним кроком необхідно зібрати інформацію про запущені Docker-контейнери, а найголовніше зібрати їх IP-адреси. Отримані IP-адреси запущених контейнерів Docker зберігаються у зміну `DOCKER_HOSTS_IPS`.

Наступним кроком треба підготувати Ansible для виконання. Створюється вказаний каталог `$SCAN_DIR` і записується конфігурація Ansible `$ANSIBLE_CONFIGURATION` у файл плейбука з назвою `playbook.yaml` у цьому каталозі. Клонується певний репозиторій GitHub `CIS-Ubuntu-20.04-Ansible`, якщо його не існує у поточному каталозі. Перевіряється версію `CIS_v1.1.0` ролі Ansible.

Наступним кроком є перебирання кожної IP-адреси хостів Docker у `DOCKER_HOSTS_IPS`. Для кожного хоста отримується ім'я контейнера, пов'язане з IP-адресою за допомогою команд Docker. Запускається контейнер Docker з ім'ям `docker-server-ssh` для роботи в якості SSH-сервера. Отримується IP-адреса контейнера SSH-сервера `SSH_SERVER_IP`. Створюється файл інвентаризації Ansible `hosts` з IP-адресою SSH-сервера. Запускається цикл для виконання сканування безпеки різних розділів (від 1 до 6) плейбука, створюючи звіти для кожного розділу. Після успішного сканування контейнер `docker-server-ssh` зупиняється.

Як фінальний крок виводиться повідомлення про те, що звіти згенеровано у вказаному каталозі `SCAN_DIR`.

Важливо зазначити, що цей скрипт спеціально розроблено для сканування Docker-контейнерів на основі бенчмарків CIS для Ubuntu 20.04. Сканування безпеки проводиться за допомогою плейбука Ansible, який включає вказані ролі та розділи.

Скрипт використовує контейнери Docker для налаштування SSH-сервера для зв'язку між Ansible і цільовими хостами. Результати сканування зберігаються в окремих файлах звітів для кожного розділу і кожного хоста Docker.

Ця програма повністю відображає розроблений алгоритм сканування і виправлення помилок у нашій Docker-інфраструктурі. Для оцінки його роботи було проведено тестування на машинах розгорнутих раніше. Процес тестування наведено в наступному підрозділі.

Розроблена програма буде використовуватись на тому самому хості де і розміщені контейнери, за цим принципом можна зобразити наступну діаграму, що зображена на рисунку 3.6.

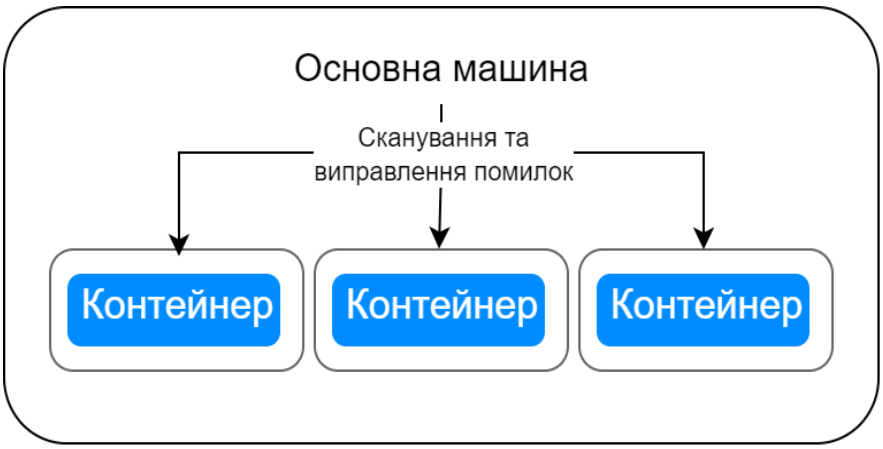


Рисунок 3.6 – Схема взаємодії використовуваних компонентів

З основної машини виправлення помилок відбувається на контейнерах, проте слід також зауважити, що комунікація відбувається через посередника, а саме SSH Docker-контейнер, що надає доступ до всіх інших контейнерів. Повна діаграма зображена на рис. 3.7.

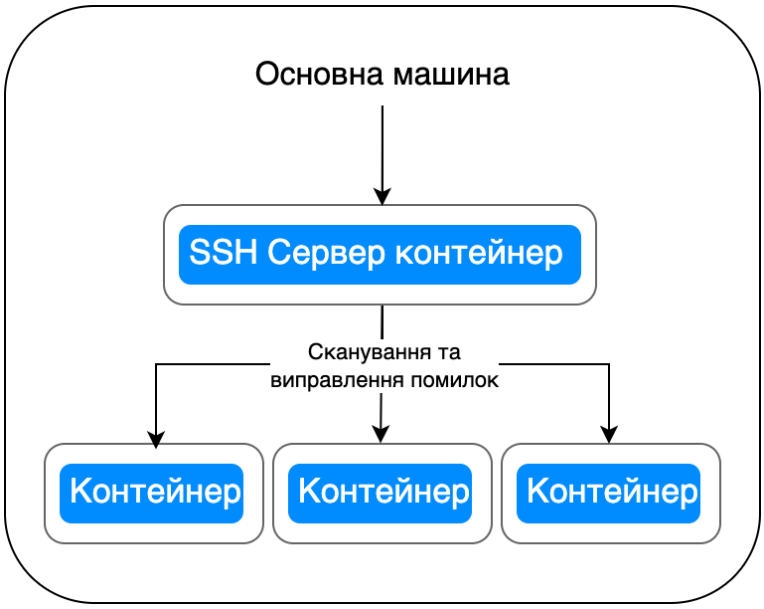


Рисунок 3.7 – Повна схема взаємодії використовуваних компонентів

Отже в цьому підрозділі було розроблено програму та розглянуто схеми взаємодії компонентів, що програма використовує.

3.2 Проведення експериментального дослідження

У попередньому розділі було розгорнуто плацдарм (середовище) для тестування, що складається з трьох контейнерів Ubuntu 20.04, що імітують справжні машини з встановленим ПЗ.

Для запуску скрипта необхідно зайти в програмну оболонку Linux або Mac та скористатися стандартною bash оболонкою.

Нижче наведено приклад запуску програми.

```
(ansible) ➜ diploma ./scan_containers.sh
HEAD is now at d537155 Merge pull request #64 from alivx/update_v1.1.0
[!] Scanning host 172.20.0.4
------------ Scanning Section 1 -------------. Done!
------------ Scanning Section 2 -------------. Done!
------------ Scanning Section 3 -------------. Done!
------------ Scanning Section 4 -------------. Done!
------------ Scanning Section 5 -------------. Done!
------------ Scanning Section 6 -------------. Done!
[!] Scanning host 172.20.0.4
------------ Scanning Section 1 -------------. Done!
------------ Scanning Section 2 -------------. Done!
------------ Scanning Section 3 -------------. Done!
------------ Scanning Section 4 -------------. Done!
------------ Scanning Section 5 -------------. Done!
```

```
------------ Scanning Section 6 -------------. Done!
[!] Scanning host 172.20.0.5
------------ Scanning Section 1 -------------. Done!
------------ Scanning Section 2 -------------. Done!
------------ Scanning Section 3 -------------. Done!
------------ Scanning Section 4 -------------. Done!
------------ Scanning Section 5 -------------. Done!
------------ Scanning Section 6 -------------. Done!
```

Після виконання програма генерує звіти по кожному хосту та секції в окремі файли. Всі звіти зберігаються у новій створеній директорії container-ansible-scan. На рис. 3.8 зображена структура даної директорії після успішного сканування.

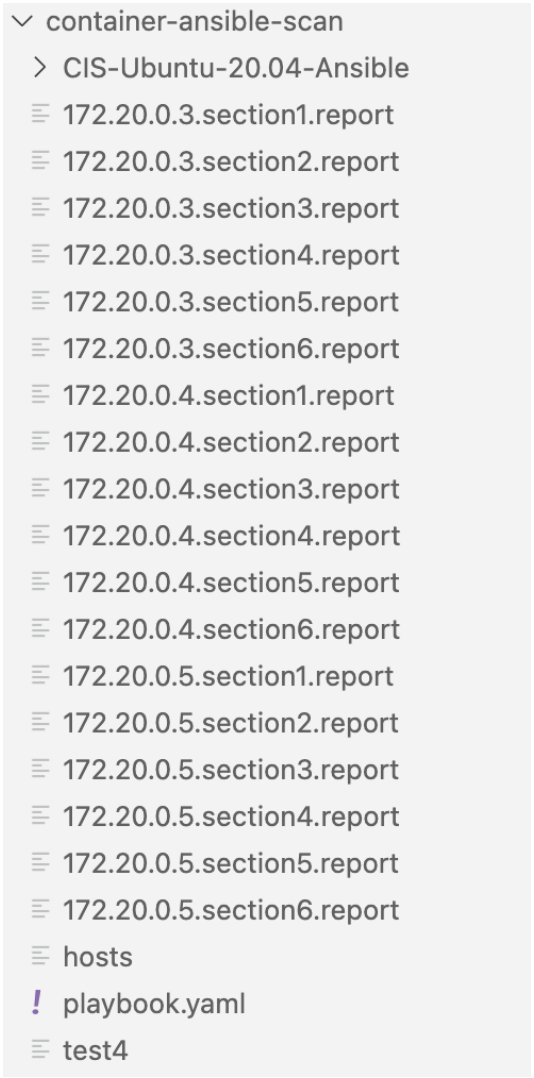


Рисунок 3.8 – Структура директорії container-ansible-scan

Кожен звіт містить в собі детальну інформацію про всі критерії безпеки, що були або просто перевірені або виправлені. Звіти названі відповідно до IP адреси

контейнера і також секції, що була просканована. Також в них міститься короткий звіт з кількістю виправлених або просканованих конфігурацій.

3.3 Порівняльна характеристика

Для оцінки ефективності метода необхідно зібрати статистику по всім секціям представленим у файлі CIS Benchmark for Ubuntu 20.04. Відкривши звіти виконання програми можна побачити статистику успішно виконаних секцій, та які критерії безпеки були впроваджені, які пропущені або скасовані через певні обставини. Відповідно даних знайдених у звітах було скомпоновано таблицю з розрахунками приросту захищеності.

Для порівняння коефіцієнту захищеності до відпрацювання створеної програми та після введемо умовні позначення $K_{\text{після}}$ та $K_{\text{до}}$.

$K_{\text{після}}$ – числове значення коефіцієнту захищеності системи після проведення сканування та виправлення помилок.

$K_{\text{до}}$ – числове значення коефіцієнту захищеності системи до проведення сканування та виправлення помилок.

Таблиця 3.1 – Розрахунки приросту коефіцієнту захищеності контейнерів

Номер секції	Позначення коефіцієнта	Розрахунки	Коефіцієнт захищеності	Приріст захищеності
Секція 1	$K_{\text{до}}$	$\frac{65}{65+34+11+3}$	$\frac{65}{113} = 0.57$	+0.3
	$K_{\text{після}}$	$\frac{65+34}{65+34+11+3}$	$\frac{99}{113} = 0.87$	

Продовження таблиці 3.1

Секція 2	$K_{\text{до}}$	$\frac{28}{28+4+10}$	$\frac{28}{42}=0.66$	+0.1
	$K_{\text{після}}$	$\frac{28+4}{28+4+10}$	$\frac{32}{42}=0.76$	
Секція 3	$K_{\text{до}}$	$\frac{38}{38+33+14}$	$\frac{38}{85}=0.44$	+0.39
	$K_{\text{після}}$	$\frac{38+33}{38+33+14}$	$\frac{71}{85}=0.83$	
Секція 4	$K_{\text{до}}$	$\frac{42}{42+37+1}$	$\frac{42}{80}=0.52$	+0.45
	$K_{\text{після}}$	$\frac{42+37}{42+37+1}$	$\frac{79}{80}=0.98$	
Секція 5	$K_{\text{до}}$	$\frac{70}{70+61+3}$	$\frac{70}{134}=0.52$	+0.45
	$K_{\text{після}}$	$\frac{70+61}{70+61+3}$	$\frac{131}{134}=0.97$	
Секція 6	$K_{\text{до}}$	$\frac{56}{56+49+6}$	$\frac{56}{111}=0.50$	+0.44
	$K_{\text{після}}$	$\frac{56+49}{56+49+6}$	$\frac{105}{111}=0.94$	

Можна побачити, що приріст безпеки у всіх секціях додатній. Щоб оцінити на скільки в середньому збільшилась захищеність системи, порахуємо середнє арифметичне коефіцієнту захищеності до та після застосування нашої програми. Варто також зазначити, що так як контейнери були запущені з одної і тої самої версії образу Ubuntu 20.04, то дані для всіх трьох аналогічні, тож таблиця 3.1 репрезентує результати для кожного контейнера.

$$K_{\text{до}} = \frac{0.57 + 0.66 + 0.44 + 0.52 + 0.52 + 0.5}{6} = 0.535$$

$$K_{\text{після}} = \frac{0.87 + 0.78 + 0.83 + 0.98 + 0.97 + 0.94}{6} = 0.894$$

Як можна побачити з підрахунків, що виконані по формулі (2.1), $K_{\text{до}}$ менше за $K_{\text{після}}$ на 0.359. Тобто загальна безпека нашого середовища відповідно до критеріїв безпеки збільшилась на майже 36%. Це гарний показник, враховуючи, що дані зміни впроваджуються автоматизованим шляхом, та за достатньо короткий проміжок часу підвищують безпеку на третину.

Для прикладу буде розглянуто певний критерій безпеки, який був застосований у наших контейнерах. Використаємо критерій під номером 6.1.11, що відповідає за те, щоб у системі не були присутні файли без власника. Ось як виглядає опис цього критерію.

```
# 6.1.11 Ensure no unowned files or directories exist
- name: 6.1.11 Ensure no unowned files or directories exist
 block:
   - name: 6.1.11 Ensure no unowned files or directories exist | Find
     shell: df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -
nouser 2> /dev/null && true || true
     register: output_6_1_11
   - name: 6.1.11 Ensure no unowned files or directories exist | Save output
     copy:
       dest: "{{ outputfiles }}/6.1.11"
       content: "{{ output_6_1_11.stdout_lines }}"
   - name: 6.1.11 Ensure no unowned files or directories exist | Fix
     file:
       path: "{{ item }}"
       owner: "{{ withoutOwnerFileDirOwner }}"
       group: "{{ withoutGroupFilesDirGroup }}"
     with_items: "{{ output_6_1_11.stdout_lines }}"
 tags:
   - section6
   - level_1_server
   - level_1_workstation
   - 6.1.11
```

Як можна побачити з опису цього критерію зо допомогою певної команди шукаються файли які не мають власника, і потім власник цих файлів змінюється на такого, який вказаний у main.yml, основній конфігурації Ansible [15].

Розроблений метод захисту буде представлено на науково-практичні інтернет-конференції "Молодь в науці: дослідження, проблеми, перспективи (МН-2024) [20].

4 ЕКОНОМІЧНА ЧАСТИНА

Виконання науково-дослідної роботи завжди передбачає отримання певних результатів і вимагає відповідних витрат. Результати виконаної роботи завжди дають нам нові знання, які в подальшому можуть бути використані для удосконалення та/або розробки (побудови) нових, більш продуктивних зразків техніки, процесів та програмного забезпечення.

Дослідження на тему «Метод підвищення захищеності Docker-контейнерів» може бути віднесено до фундаментальних і пошукових наукових досліджень і спрямоване на вирішення наукових проблем, пов’язаних з практичним застосуванням. Основою таких досліджень є науковий ефект, який виражається в отриманні наукових результатів, які збільшують обсяг знань про природу, техніку та суспільство, які розвивають теоретичну базу в тому чи іншому науковому напрямку, що дозволяє виявити нові закономірності, які можуть використовуватися на практиці.

Для цього випадку виконаємо такі етапи робіт:

1) здійснимо проведення наукового аудиту досліджень, тобто встановлення їх наукового рівня та значимості;

2) проведемо планування витрат на проведення наукових досліджень;

3) здійснимо розрахунок рівня важливості наукового дослідження та перспективності, визначимо ефективність наукових досліджень.

4.1 Оцінювання наукового ефекту

Основними ознаками наукового ефекту науково-дослідної роботи є новизна роботи, рівень її теоретичного опрацювання, перспективність, рівень розповсюдження результатів, можливість реалізації [17]. Науковий ефект НДР на тему «Метод підвищення захищеності Docker-контейнерів» можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Значення показників ступеня новизни і рівня теоретичного опрацювання науково-дослідної роботи в балах наведені в табл. 4.1 та 4.2.

Таблиця 4.1 – Показники ступеня новизни науково-дослідної роботи виставлені експертами

Ступінь новизни	Характеристика ступеня новизни	Значення ступеня новизни, бали		
		Експерти (ПІБ, посада)		
		1	2	3
Принципово нова	Робота якісно нова за постановкою задачі і ґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отримані принципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод	0	0	0
Нова	Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів	54	60	59
Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв’язок (або знайдено новий зв’язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об’єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональна модифікація (з ознаками новизни)	0	0	0
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим	0	0	0
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам	0	0	0
Середнє значення балів експертів		57,7		

Згідно отриманого середнього значення балів експертів ступінь новизни характеризується як нова, тобто отримана нова інформація, яка суттєво зменшує невизначеність наявних знань (по-новому або вперше пояснені відомі факти,

закономірності, впроваджені нові поняття, розкрита структура змісту) та проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів.

Таблиця 4.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи виставлені експертами

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Експерт (ПІБ, посада)		
	1	2	3
Відкриття закону, розробка теорії	0	0	0
Глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	67	68	65
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	0	0	0
Елементарний аналіз зв'язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо	0	0	0
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	0	0	0
Середнє значення балів експертів	66,7		

Згідно отриманого середнього значення балів експертів рівень теоретичного опрацювання науково-дослідної роботи характеризується як глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу.

Показник, який характеризує рівень наукового ефекту, визначаємо за формулою [22]:

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор}, \quad (4.1)$$

де $k_{нов}, k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{нов} = 57,7, k_{теор} = 66,7$ балів;

0,6 та 0,4 – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор} = 0,6 \cdot 57,7 + 0,4 \cdot 66,67 = 61,27 \text{ балів.}$$

Визначення характеристики показника $E_{нау}$ проводиться на основі висновків експертів виходячи з граничних значень, які наведені в табл. 4.3.

Таблиця 4.3 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Відповідно до визначеного рівня наукового ефекту проведеної науково-дослідної роботи на тему «Метод підвищення захищеності Docker-контейнерів», даний рівень становить 61,27 балів і відповідає статусу - середній рівень. Тобто у даному випадку можна вести мову про потенційну фактичну ефективність науково-дослідної роботи.

4.2 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Метод підвищення захищеності Docker-контейнерів», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.2.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп,

науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [22]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \quad (4.2)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=21 дні.

$$З_о = 17400{,}00 \cdot 21 / 21 = 17400{,}00 \; грн.$$

Проведені розрахунки зведемо до таблиці 4.4.

Таблиця 4.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	17400,00	828,57	21	17400,00
Науковий співробітник	17150,00	816,67	12	9800,00
Інженер-програміст 1-ї категорії	17050,00	811,90	21	17050,00
Лаборант	6750,00	321,43	10	3214,29
Всього				47464,29

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Метод підвищення захищеності Docker-контейнерів» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i , \tag{4.3}$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} , \tag{4.4}$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [22];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$$C_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}65 / (21 \cdot 8) = 72{,}38 \ грн.$$

$$З_{р1} = 72{,}38 \cdot 10{,}50 = 760{,}03 \ грн.$$

Таблиця 4.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Встановлення допоміжного обладнання	10,50	2	1,10	72,38	760,03
Інсталяція програмного забезпечення	6,25	3	1,35	88,83	555,22
Встановлення цифрових обчислювальних систем	5,15	5	1,70	111,87	576,11
Відлагодження програмних модулів аналізу даних	5,75	4	1,50	98,71	567,56
Підготовка дослідження	9,12	4	1,50	98,71	900,19
Формування бази даних результатів дослідження	16,00	2	1,10	72,38	1158,14
Всього					4517,25

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.5)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$З_{дод}$ = (47464,29 + 4517,25) · 11 / 100% = 5717,97 грн.

4.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad , \tag{4.6}$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (47464,29 + 4517,25 + 5717,97) · 22 / 100% = 12693,89 грн.

4.2.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Метод підвищення захищеності Docker-контейнерів».

Витрати на матеріали на даному етапі проведення досліджень в основному пов’язані з використанням моделей елементів та моделювання роботи і досліджень за допомогою комп’ютерної техніки та створення експериментальних математичних моделей або програмного забезпечення, тому дані витрати формуються на основі витратних матеріалів характерних для офісних робіт.

Витрати на матеріали ($М$), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$М = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц_{в\,j} \, , \tag{4.7}$$

де $Н_j$ – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 … 1,15*);

$В_j$ – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, грн/кг.

$M_1 = 2,0 \cdot 225,00 \cdot 1,1 - 0 \cdot 0 = 495,00$ *грн.*

Проведені розрахунки зведемо до таблиці 4.6.

Таблиця 4.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір канцелярський офісний (А4)	225,00	2,0	0	0	495,00
Папір для заміток (А5)	116,00	4,0	0	0	510,40
Начиння канцелярське	195,00	3,0	0	0	643,50
Органайзер офісний	183,00	3,0	0	0	603,90
Картридж для принтера	950,00	1,0	0	0	1045,00
Всього					3297,80

4.2.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Метод підвищення захищеності Docker-контейнерів», розраховуємо, згідно з їхньою номенклатурою, за формулою:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (4.8)$$

де $Н_j$ – кількість комплектуючих *j*-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих *j*-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j = 1,1 \ldots 1,15$).

$К_в = 1 \cdot 3079,00 \cdot 1,1 = 3386,90$ *грн.*

Проведені розрахунки зведемо до таблиці 4.7.

Таблиця 4.7 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Зовнішній жорсткий диск 2.5" 2TB Seagate (STGD2000200)	1	3079,00	3386,90
Миша бездротова Logitech M185 WL Swift Grey 910-002238	1	754,00	829,40
Всього			4216,30

4.2.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення.

Балансову вартість спецустаткування розраховуємо за формулою:

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \ , \qquad (4.9)$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, грн;

$C_{пр.i}$ –кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань устаткування.

$B_{спец} = 75563,00 \cdot 1 \cdot 1,1 = 83119,30$ *грн.*

Отримані результати зведемо до таблиці 4.8.

4.2.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Таблиця 4.8 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Ноутбук Apple MacBook Pro 16 Retina, Silver 512GB (MVVL2) 2019. Intel Core i7	1	75 563,00	83119,30
AWS Cloud Computing. Хмарні обчислення. Віртуальні машини Ubuntu 20.04	2	646,00	1421,20
Всього			84540,50

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (4.10)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань програмних засобів.

$B_{прг} = 7910,00 \cdot 1 \cdot 1,1 = 8701,00$ *грн.*

Отримані результати зведемо до таблиці 4.9.

Таблиця 4.9 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Прикладне програмне забезпечення розробки системи аналізу	1	7910,00	8701,00
Всього			8701,00

4.2.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (35830,00 \cdot 1) / (2 \cdot 12) = 1492,92$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Програмно-обчислювальний комплекс розробки системи аналізу даних	35830,00	2	1	1492,92
Місце оператора спеціалізоване	8200,00	5	1	136,67
Офісна оргтехніка	9600,00	4	1	200,00
Дослідницька лабораторія	500000,00	20	1	2083,33
Всього				3912,92

4.2.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.12)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e$ = 7,20 грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0,05 \cdot 200,0 \cdot 7,20 \cdot 0,95 / 0,97 = 72,00$ грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.11 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Ноутбук Apple MacBook Pro 16 Retina, Silver 512GB (MVVL2) 2019. Intel Core i7	0,05	200,0	72,00
Програмно-обчислювальний комплекс розробки системи аналізу даних	0,42	200,0	604,80
Місце оператора спеціалізоване	0,10	200,0	144,00
Офісна оргтехніка	0,60	5,0	21,60
Всього			824,40

4.2.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Метод підвищення захищеності Docker-контейнерів» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а також

витрати на відрядження на наукові з'їзди, конференції, наради, пов'язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \quad (4.13)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 20%.

$$B_{св} = (47464,29 + 4517,25) \cdot 20 / 100\% = 10396,31 \text{ грн.}$$

4.2.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» відсутні.

4.2.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.14)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 70%.

$$I_в = (47464,29 + 4517,25) \cdot 70 / 100\% = 36387,08 \text{ грн.}$$

4.2.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.15)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 100%.

$B_{нзв}$ = (47464,29 + 4517,25) · 100 / 100% = 51981,54 грн.

Витрати на проведення науково-дослідної роботи на тему «Метод підвищення захищеності Docker-контейнерів» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + B_{спец} + B_{прг} + A_{обл} + B_е + B_{св} + B_{сп} + I_в + B_{нзв}. \quad (4.16)$$

$B_{заг}$= 47464,29 +4517,25 +5717,97 +12693,89118 +3297,80 +4216,30 + 84540,50 + 8701,00 + 3912,92 +725,40 +10396,31 +0,00 +36387,08 +51981,54 = 274651,23 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.17)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η =0,95.

ЗВ = 274651,23 / 0,95 = 289106,56 грн.

4.3 Оцінювання важливості та наукової значимості науково-дослідної роботи

Оцінювання та доведення ефективності виконання науково-дослідної роботи фундаментального чи пошукового характеру є достатньо складним процесом і часто базується на експертних оцінках, тому має вірогідний характер.

Для обґрунтування доцільності виконання науково-дослідної роботи на тему «Метод підвищення захищеності Docker-контейнерів» використовується спеціальний комплексний показник, що враховує важливість, результативність роботи, можливість впровадження її результатів у виробництво, величину витрат на роботу.

Комплексний показник K_P рівня науково-дослідної роботи може бути розрахований за формулою:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \tag{4.18}$$

де I – коефіцієнт важливості роботи. Приймемо $I = 4$;

n – коефіцієнт використання результатів роботи; $n = 0$, коли результати роботи не будуть використовуватись; $n = 1$, коли результати роботи будуть використовуватись частково; $n = 2$, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках; $n = 3$, коли результати можуть використовуватись навіть без проведення дослідно-конструкторських розробок. Приймемо $n=2$;

T_C – коефіцієнт складності роботи. Приймемо $T_C = 3$;

R – коефіцієнт результативності роботи; якщо результати роботи плануються вище відомих, то $R = 4$; якщо результати роботи відповідають відомому рівню, то $R = 3$; якщо нижче відомих результатів, то $R = 1$. Приймемо $R = 4$;

B – вартість науково-дослідної роботи, тис. грн. Приймемо B =245702,88 грн;

t – час проведення дослідження. Приймемо t = 0,08 років, (1 міс.).

Визначення показників *I, n, T_C, R, B, t* здійснюється експертним шляхом або на основі нормативів [22].

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t} = 4^2 \cdot 3 \cdot 4 \,/\, 245{,}7 \cdot 0{,}08 = 9{,}38.$$

Якщо $K_P > 1$, то науково-дослідну роботу на тему «Метод підвищення захищеності Docker-контейнерів» можна вважати ефективною з високим науковим, технічним і економічним рівнем.

Витрати на проведення науково-дослідної роботи на тему «Метод підвищення захищеності Docker-контейнерів» складають 245702,88 грн. Відповідно до проведеного аналізу та розрахунків рівень науково-економічного ефекту проведеної науково-дослідної роботи на тему «Метод підвищення захищеності Docker-контейнерів» є середній, а дослідження актуальними, рівень доцільності виконання науково-дослідної роботи $K_P > 1$, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

ВИСНОВКИ

В магістерській кваліфікаційній роботі було проведено комплексний аналіз стану безпеки Docker з метою зміцнення контейнерних середовищ. Дослідження було зосереджено на розробці системного підходу до посилення безпеки контейнерів Docker, використовуючи автоматизацію Ansible і дотримуючись Центру інтернет-безпеки CIS Ubuntu Benchmark версії 20.04.

Перший етап дослідження включав ретельне вивчення існуючих заходів безпеки Docker, виявлення потенційних вразливостей та оцінку загального стану безпеки контейнерних розгортань. Цей аналіз заклав основу для розробки методу усунення прогалин у безпеці та підвищення надійності контейнерів Docker.

Основний метод була зосереджена на інтеграції Ansible, потужного інструменту автоматизації, та CIS Ubuntu Benchmark v20.04. Плейбуки Ansible були використані для автоматизації впровадження засобів контролю безпеки, дотримання найкращих практик та коригування конфігурації в контейнерах Docker. Також було використано bash для автоматизації процесів. CIS Ubuntu Benchmark v20.04 містить повний набір рекомендацій і тестів, які слугують орієнтиром для встановлення безпечної базової конфігурації.

Для перевірки ефективності запропонованого методу було виконано практичне впровадження та ретельне тестування. Рішення передбачало розгортання плейбуків Ansible у контейнерах Docker, застосування рекомендованих конфігурацій безпеки та оцінку результатів у порівнянні з попередньо визначеними критеріями безпеки. За допомогою тестування дослідження було продемонстровано ефективність розробленого рішення для зменшення ризиків безпеки та покращення загального стану безпеки контейнерів Docker.

Таким чином, у цій роботі було проаналізовано ландшафт безпеки Docker, але й запропоновано практичну метод для підвищення безпеки контейнерів за допомогою інтеграції автоматизації Ansible та CIS Ubuntu Benchmark v20.04.

Результати етапу тестування надали докази ефективності рішення для досягнення підвищення захищеності в середовищах з використанням Docker-контейнерів. Також було проаналізовано та представлено доцільність та ефективність економічної складової роботи.

Результати представлені в цьому дослідженні, пропонують цінну інформацію для організацій, які прагнуть підвищити безпеку своїх контейнерних додатків, зберігаючи при цьому відповідність встановленим критеріям і кращим практикам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Docker Security Documentation. URL: https://docs.docker.com/engine/security/ (дата звернення: 10.09.2023)
2. Top 22 Docker Security Best Practices, Ultimate Guide. URL: https://blog.aquasec.com/docker-security-best-practices (дата звернення: 19.09.2023)
3. Security for Containers and Kubernetes. Luigi Aversa. (дата звернення 21.09.2023)
4. Runtime options with Memory, CPUs, and GPUs. URL: https://docs.docker.com/config/containers/resource_constraints/ (дата звернення 2.10.2023)
5. Half of 4 Million Public Docker Hub Images Found to Have Critical Vulnerabilities. URL: https://www.infoq.com/news/2020/12/dockerhub-image -vulnerabilities/ (дата звернення 05.10.2023)
6. NIST SP 800-190. Application Container Security Guide. URL: https://csrc.nist.gov/pubs/sp/800/190/final (дата звернення 09.10.2023)
7. Getting started with Clair. URL: https://quay.github.io/clair/howto/ getting_started.html (дата звернення 10.10.2023)
8. OpenShift Container Platform security and compliance. URL: https://docs.openshift.com/container-platform/4.10/security/ (дата звернення 13.10.2023)
9. CIS Benchmark for Ubuntu 20.04. URL: https://www.cisecurity.org/benchmark /docker (дата звернення 15.10.2023)
10. Trivy. Сканер образів Docker-контейнерів. URL: https://www.aquasec.com/ products/trivy/ (дата звернення 18.10.2023)
11. Ansible documentation. URL: https://docs.ansible.com/ansible/latest/ getting_started/index.html (дата звернення 24.10.2023)
12. Git репозиторій для Ansible. Ansible + CIS Ubuntu v20.04 Benchmark. URL: https://github.com/alivx/CIS-Ubuntu-20.04-Ansible (дата звернення 25.10.2023)

13. Docker SSH Server для підключення до контейнерів застосунків. URL: https://github.com/maxivak/docker-ssh (дата звернення 01.11.2023)
14. Python documentation. How to use. URL: https://www.python.org/doc/ (дата звернення 10.11.2023)
15. What Is Ansible? Uses, Working, Architecture, Features. URL: https://www.spiceworks.com/tech/devops/articles/what-is-ansible/ (дата звернення 16.11.2023)
16. Козачок В. О., Лукічов В. В. Метод підвищення захищеності docker-контейнерів Матеріали Всеукраїнської науково-практичної інтернет-конференції Молодь в науці: дослідження, проблеми, перспективи (МН-2024), Вінниця, 11-20 травня 2024 р. [Електронний ресурс] URL: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/view/19774
17. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

ДОДАТКИ

75

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ
МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Метод підвищення захищеності Docker-контейнерів.

Автор роботи: Козачок Вячеслав Олександрович

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 91,08 %. Схожість – 8,92 %.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

• 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

• 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку (підпис) Валентина КАПЛУН

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи (підпис) Вячеслав КОЗАЧОК

Керівник роботи (підпис) Віталій ЛУКІЧОВ

Додаток Б

Код розробленого програмного застосунку

```
SCAN_DIR="./container-ansible-scan"

ANSIBLE_CONFIGURATION=$(cat << EOF
- name: CIS
 hosts: myhosts
 become: yes
 remote_user: ubuntu
 gather_facts: no
 roles:
   - { role: "CIS-Ubuntu-20.04-Ansible" }

EOF
)

DOCKER_HOSTS_IPS=$(docker ps -q | xargs -n 1 docker inspect \
   --format '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' \
   | sed 's#^/##')

# Prepare Ansible configuration
mkdir -p $SCAN_DIR

echo "$ANSIBLE_CONFIGURATION" > $SCAN_DIR/playbook.yaml

cd "$SCAN_DIR"
if [ ! -d "./CIS-Ubuntu-20.04-Ansible" ]; then
   git clone https://github.com/alivx/CIS-Ubuntu-20.04-Ansible.git
fi

cd CIS-Ubuntu-20.04-Ansible
git checkout CIS_v1.1.0
cd ../../

for ip in DOCKER_HOSTS_IPS
do
   echo "[!] Scanning host $ip"

   CONTAINER_NAME=$(docker ps -q | xargs -n 1 docker inspect --format '{{range
.NetworkSettings.Networks}}{{.IPAddress}}{{end}} {{.Name}}' | grep $ip | awk -F
'/' '{ print $2 }')
   SSH_CONTAINER_NAME="docker-server-ssh"
   docker run -d --rm -p 2222:22 \
           -v /var/run/docker.sock:/var/run/docker.sock \
           -e FILTERS='{\"name\":[\"^/${SSH_CONTAINER_NAME}$\"]}' -e
AUTH_MECHANISM=noAuth \
           --name $SSH_CONTAINER_NAME jeroenpeeters/docker-ssh

   SSH_SERVER_IP=$(docker inspect --format '{{range
.NetworkSettings.Networks}}{{.IPAddress}}{{end}}' $SSH_CONTAINER_NAME)

   ANSIBLE_INVENTORY="[myhosts]\n$SSH_SERVER_IP"

   echo $ANSIBLE_INVENTORY > "$SCAN_DIR/hosts"

   cd $SCAN_DIR

   for i in {1..6}
```

```
   do
       echo "------------ Scanning Section $i -------------"

       ansible-playbook -i hosts playbook.yaml -t section$i  -v | tee
$CONTAINER_NAME.$ip.section$i.report


       echo "Done!"

   done

   docker stop docker-server-ssh
   sleep(1)
done

      echo Reports are generated in the $SCAN_DIR.
```

Додаток В

Результат сканування секції №1 в контейнері

```
PLAY [CIS] *********************************************************************

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.1 Ensure mounting of cramfs filesystems is disabled] ***
ok: [172.20.0.4] => {"ansible_facts": {"discovered_interpreter_python": "/usr/bin/python3"},
"backup": "", "changed": false, "msg": ""}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.1 Ensure mounting of cramfs filesystems is disabled |
modprobe] ***
ok: [172.20.0.4] => {"changed": false, "name": "cramfs", "params": "", "state": "absent"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.2 Ensure mounting of freevxfs filesystems is disabled] ***
ok: [172.20.0.4] => {"backup": "", "changed": false, "msg": ""}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.2 Ensure mounting of freevxfs filesystems is disabled |
modprobe] ***
ok: [172.20.0.4] => {"changed": false, "name": "freevxfs", "params": "", "state": "absent"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.3 Ensure mounting of jffs2 filesystems is disabled] ***
ok: [172.20.0.4] => {"backup": "", "changed": false, "msg": ""}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.3 Ensure mounting of jffs2 filesystems is disabled] ***
ok: [172.20.0.4] => {"changed": false, "name": "jffs2", "params": "", "state": "absent"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.4 Ensure mounting of hfs filesystems is disabled] ***
changed: [172.20.0.4] => {"backup": "", "changed": true, "msg": "line added"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.4 Ensure mounting of hfs filesystems is disabled |
modprobe] ***
ok: [172.20.0.4] => {"changed": false, "name": "hfs", "params": "", "state": "absent"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.5 Ensure mounting of hfsplus filesystems is disabled] ***
changed: [172.20.0.4] => {"backup": "", "changed": true, "msg": "line added"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.5 Ensure mounting of hfsplus filesystems is disabled |
modprobe] ***
ok: [172.20.0.4] => {"changed": false, "name": "hfsplus", "params": "", "state": "absent"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.6 Ensure mounting of squashfs filesystems is disabled] ***
skipping: [172.20.0.4] => {"changed": false, "skip_reason": "Conditional result was False"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.6 Ensure mounting of squashfs filesystems is disabled |
modprobe] ***
skipping: [172.20.0.4] => {"changed": false, "skip_reason": "Conditional result was False"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.7 Ensure mounting of udf filesystems is disabled] ***
changed: [172.20.0.4] => {"backup": "", "changed": true, "msg": "line added"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.7 Ensure mounting of udf filesystems is disabled |
modprobe] ***
ok: [172.20.0.4] => {"changed": false, "name": "udf", "params": "", "state": "absent"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.7 Ensure mounting of FAT filesystems is limited] ***
changed: [172.20.0.4] => {"backup": "", "changed": true, "msg": "line added"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.7 Ensure mounting of FAT filesystems is limited | modprobe]
***
fatal: [172.20.0.4]: FAILED! => {"changed": false, "msg": "modprobe: FATAL: Module vfat is
builtin.\n", "name": "vfat", "params": "", "rc": 1, "state": "absent", "stderr": "modprobe: FATAL:
Module vfat is builtin.\n", "stderr_lines": ["modprobe: FATAL: Module vfat is builtin."],
"stdout": "", "stdout_lines": []}
...ignoring
```

```
TASK [CIS-Ubuntu-20.04-Ansible : 1.1.2 Ensure /tmp is configured] **************
changed: [172.20.0.4] => {"changed": true, "checksum": "996d1da8dccde51f23657745a2feb2f5b4ee3e69", "dest": "/etc/systemd/system/tmp.mount", "gid": 0, "group": "root", "md5sum": "d5f00e8f3f8a3a820ec32e102f57716b", "mode": "0644", "owner": "root", "size": 805, "src": "/usr/share/systemd/tmp.mount", "state": "file", "uid": 0}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.2 Ensure /tmp is configured | edit file] ***
changed: [172.20.0.4] => {"backup": "", "changed": true, "msg": "line replaced"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.2 Ensure /tmp is configured | reload demon] ***
ok: [172.20.0.4] => {"changed": false, "name": null, "status": {}}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.2 Ensure /tmp is configured | enable and start tmp.mount] ***
changed: [172.20.0.4] => {"changed": true, "enabled": true, "name": "tmp.mount", "state": "started", "status": {"ActiveEnterTimestampMonotonic": "0", "ActiveExitTimestampMonotonic": "0", "ActiveState": "inactive", "After": "-.mount system.slice systemd-journald.socket swap.target", "AllowIsolate": "no", "AllowedCPUs": "", "AllowedMemoryNodes": "", "AmbientCapabilities": "", "AssertResult": "no", "AssertTimestampMonotonic": "0", "Before": "local-fs.target e2scrub_reap.service basic.target logrotate.service systemd-resolved.service open-vm-tools.service systemd-logind.service systemd-timesyncd.service umount.target ModemManager.service", "BlockIOAccounting": "no", "BlockIOWeight": "[not set]", "CPUAccounting": "no", "CPUAffinity": "", "CPUAffinityFromNUMA": "no", "CPUQuotaPerSecUSec": "infinity", "CPUQuotaPeriodUSec": "infinity", "CPUSchedulingPolicy": "0", "CPUSchedulingPriority": "0", "CPUSchedulingResetOnFork": "no", "CPUShares": "[not set]", "CPUUsageNSec": "[not set]", "CPUWeight": "[not set]", "CacheDirectoryMode": "0755", "CanIsolate": "no", "CanReload": "yes", "CanStart": "yes", "CanStop": "yes", "CapabilityBoundingSet": "cap_chown cap_dac_override cap_dac_read_search cap_fowner cap_fsetid cap_kill cap_setgid cap_setuid cap_setpcap cap_linux_immutable cap_net_bind_service cap_net_broadcast cap_net_admin cap_net_raw cap_ipc_lock cap_ipc_owner cap_sys_module cap_sys_rawio cap_sys_chroot cap_sys_ptrace cap_sys_pacct cap_sys_admin cap_sys_boot cap_sys_nice cap_sys_resource cap_sys_time cap_sys_tty_config cap_mknod cap_lease cap_audit_write cap_audit_control cap_setfcap cap_mac_override cap_mac_admin cap_syslog cap_wake_alarm cap_block_suspend cap_audit_read 0x26 0x27 0x28", "CollectMode": "inactive", "ConditionResult": "no", "ConditionTimestampMonotonic": "0", "ConfigurationDirectoryMode": "0755", "Conflicts": "umount.target", "ControlPID": "0", "DefaultDependencies": "no", "DefaultMemoryLow": "0", "DefaultMemoryMin": "0", "Delegate": "no", "Description": "Temporary Directory (/tmp)", "DevicePolicy": "auto", "DirectoryMode": "0755", "Documentation": "https://systemd.io/TEMPORARY_DIRECTORIES man:file-hierarchy(7) https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems", "DynamicUser": "no", "EffectiveCPUs": "", "EffectiveMemoryNodes": "", "FailureAction": "none", "FinalKillSignal": "9", "ForceUnmount": "no", "FragmentPath": "/etc/systemd/system/tmp.mount", "GID": "[not set]", "IOAccounting": "no", "IOReadBytes": "18446744073709551615", "IOReadOperations": "18446744073709551615", "IOSchedulingClass": "0", "IOSchedulingPriority": "0", "IOWeight": "[not set]", "IOWriteBytes": "18446744073709551615", "IOWriteOperations": "18446744073709551615", "IPAccounting": "no", "IPEgressBytes": "[no data]", "IPEgressPackets": "[no data]", "IPIngressBytes": "[no data]", "IPIngressPackets": "[no data]", "Id": "tmp.mount", "IgnoreOnIsolate": "yes", "IgnoreSIGPIPE": "yes", "InactiveEnterTimestampMonotonic": "0", "InactiveExitTimestampMonotonic": "0", "JobRunningTimeoutUSec": "infinity", "JobTimeoutAction": "none", "JobTimeoutUSec": "infinity", "KeyringMode": "shared", "KillMode": "control-group", "KillSignal": "15", "LazyUnmount": "no", "LimitAS": "infinity", "LimitASSoft": "infinity", "LimitCORE": "infinity", "LimitCORESoft": "0", "LimitCPU": "infinity", "LimitCPUSoft": "infinity", "LimitDATA": "infinity", "LimitDATASoft": "infinity", "LimitFSIZE": "infinity", "LimitFSIZESoft": "infinity", "LimitLOCKS": "infinity", "LimitLOCKSSoft": "infinity", "LimitMEMLOCK": "65536", "LimitMEMLOCKSoft": "65536", "LimitMSGQUEUE": "819200", "LimitMSGQUEUESoft": "819200", "LimitNICE": "0", "LimitNICESoft": "0", "LimitNOFILE": "524288", "LimitNOFILESoft": "1024", "LimitNPROC": "3754", "LimitNPROCSoft": "3754", "LimitRSS": "infinity", "LimitRSSSoft": "infinity", "LimitRTPRIO": "0", "LimitRTPRIOSoft": "0", "LimitRTTIME": "infinity", "LimitRTTIMESoft": "infinity", "LimitSIGPENDING": "3754", "LimitSIGPENDINGSoft": "3754", "LimitSTACK": "infinity", "LimitSTACKSoft": "8388608", "LoadState": "loaded", "LockPersonality": "no", "LogLevelMax": "-1", "LogRateLimitBurst": "0", "LogRateLimitIntervalUSec": "0", "LogsDirectoryMode": "0755", "MemoryAccounting": "yes", "MemoryCurrent": "[not set]", "MemoryDenyWriteExecute": "no", "MemoryHigh": "infinity", "MemoryLimit": "infinity", "MemoryLow": "0", "MemoryMax": "infinity", "MemoryMin": "0", "MemorySwapMax": "infinity", "MountAPIVFS": "no", "MountFlags": "", "NUMAMask": "", "NUMAPolicy": "n/a", "Names": "tmp.mount", "NeedDaemonReload": "no", "Nice": "0", "NoNewPrivileges": "no", "NonBlocking": "no", "OOMScoreAdjust": "0", "OnFailureJobMode": "replace", "Options": "mode=1777,strictatime,nosuid,nodev,noexec,size=1G", "Perpetual": "no", "PrivateDevices": "no",
```

"PrivateMounts": "no", "PrivateNetwork": "no", "PrivateTmp": "no", "PrivateUsers": "no", "ProtectControlGroups": "no", "ProtectHome": "no", "ProtectHostname": "no", "ProtectKernelLogs": "no", "ProtectKernelModules": "no", "ProtectKernelTunables": "no", "ProtectSystem": "no", "RefuseManualStart": "no", "RefuseManualStop": "no", "RemoveIPC": "no", "RequiredBy": "systemd-timesyncd.service e2scrub_reap.service systemd-resolved.service ModemManager.service logrotate.service systemd-logind.service open-vm-tools.service", "Requires": "-.mount system.slice", "RequiresMountsFor": "/", "RestartKillSignal": "15", "RestrictNamespaces": "no", "RestrictRealtime": "no", "RestrictSUIDSGID": "no", "Result": "success", "RuntimeDirectoryMode": "0755", "RuntimeDirectoryPreserve": "no", "SameProcessGroup": "yes", "SecureBits": "0", "SendSIGHUP": "no", "SendSIGKILL": "yes", "Slice": "system.slice", "SloppyOptions": "no", "StandardError": "inherit", "StandardInput": "null", "StandardInputData": "", "StandardOutput": "journal", "StartLimitAction": "none", "StartLimitBurst": "5", "StartLimitIntervalUSec": "10s", "StartupBlockIOWeight": "[not set]", "StartupCPUShares": "[not set]", "StartupCPUWeight": "[not set]", "StartupIOWeight": "[not set]", "StateChangeTimestamp": "Sat 2023-12-09 15:35:11 UTC", "StateChangeTimestampMonotonic": "43447561", "StateDirectoryMode": "0755", "StopWhenUnneeded": "no", "SubState": "dead", "SuccessAction": "none", "SyslogFacility": "3", "SyslogLevel": "6", "SyslogLevelPrefix": "yes", "SyslogPriority": "30", "SystemCallErrorNumber": "0", "TTYReset": "no", "TTYVHangup": "no", "TTYVTDisallocate": "no", "TasksAccounting": "yes", "TasksCurrent": "[not set]", "TasksMax": "1126", "TimeoutCleanUSec": "infinity", "TimeoutUSec": "1min 30s", "TimerSlackNSec": "50000", "Transient": "no", "Type": "tmpfs", "UID": "[not set]", "UMask": "0022", "UnitFilePreset": "enabled", "UnitFileState": "disabled", "UtmpMode": "init", "WantedBy": "basic.target", "WatchdogSignal": "6", "What": "tmpfs", "Where": "/tmp"}}

```
TASK [CIS-Ubuntu-20.04-Ansible : 1.1.6 Ensure /dev/shm is configured
1.1.7 Ensure nodev option set on /dev/shm partition
1.1.8 Ensure nosuid option set on /dev/shm partition
1.1.9 Ensure noexec option set on /dev/shm partition] ***
```

changed: [172.20.0.4] => {"backup_file": "", "boot": "yes", "changed": true, "dump": "0", "fstab": "/etc/fstab", "fstype": "tmpfs", "name": "/dev/shm", "opts": "defaults,nodev,nosuid,noexec", "passno": "0", "src": "tmpfs"}

```
TASK [CIS-Ubuntu-20.04-Ansible : 1.1.10 Ensure separate partition exists for /var] ***
ok: [172.20.0.4] => {
   "msg": "during setup step\nFor new installations, during installation create a custom partition setup and specify a\nseparate partition for /var .\nFor systems that were previously installed, create a new partition and configure\n/etc/fstab as appropriate."
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.12 Ensure nodev option set on /var/tmp partitions] ***
```

changed: [172.20.0.4] => {"changed": true, "cmd": "mount | grep \"on /var/tmp\" && true || true\n", "delta": "0:00:00.005782", "end": "2023-12-09 16:04:40.062983", "msg": "", "rc": 0, "start": "2023-12-09 16:04:40.057201", "stderr": "", "stderr_lines": [], "stdout": "", "stdout_lines": []}

```
TASK [CIS-Ubuntu-20.04-Ansible : /var/tmp partitions] *************************
ok: [172.20.0.4] => {
   "msg": []
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.15 Ensure separate partition exists for /var/log] ***
ok: [172.20.0.4] => {
   "msg": "For new installations, during installation create a custom partition setup and specify a separate partition"
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.16 Ensure separate partition exists for /var/log/audit] ***
ok: [172.20.0.4] => {
   "msg": "For new installations, during installation create a custom partition setup and specify a separate partition"
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.17 Ensure separate partition exists for /home] ***
ok: [172.20.0.4] => {
   "msg": "For new installations, during installation create a custom partition setup and specify a separate partition"
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.18 Ensure nodev option set on /home partition] ***
```

```
ok: [172.20.0.4] => {
   "msg": "For new installations, during installation create a custom partition setup and specify
a separate partition"
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.19 Ensure nodev option set on removable media partitions]
***
ok: [172.20.0.4] => {
   "msg": "For new installations, during installation create a custom partition setup and specify
a separate partition"
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.20 Ensure nosuid option set on removable media partitions]
***
ok: [172.20.0.4] => {
   "msg": "For new installations, during installation create a custom partition setup and specify
a separate partition"
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.21 Ensure noexec option set on removable media partitions]
***
ok: [172.20.0.4] => {
   "msg": "For new installations, during installation create a custom partition setup and specify
a separate partition"
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.22 Ensure sticky bit is set on all world-writable directories
| get info] ***
changed: [172.20.0.4] => {"changed": true, "cmd": "df --local -P | awk '{if (NR!=1) print $6}' |
xargs -I '{}' find '{}' -xdev -type d \\( -perm -0002 -a ! -perm -1000 \\) 2>/dev/null\n",
"delta": "0:00:03.347229", "end": "2023-12-09 16:04:44.961464", "msg": "", "rc": 0, "start":
"2023-12-09 16:04:41.614235", "stderr": "", "stderr_lines": [], "stdout": "", "stdout_lines": []}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.22 Ensure sticky bit is set on all world-writable directories
| fix] ***
skipping: [172.20.0.4] => {"changed": false, "skip_reason": "Conditional result was False"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.23 Disable Automounting | service disable] ***
fatal: [172.20.0.4]: FAILED! => {"changed": false, "msg": "Could not find the requested service
autofs: host"}
...ignoring

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.23 Disable Automounting | package remove] ***
ok: [172.20.0.4] => {"changed": false}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.24 Disable USB Storage | modprobe] ********
changed: [172.20.0.4] => {"backup": "", "changed": true, "msg": "line added"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.24 Disable USB Storage] ******************
ok: [172.20.0.4] => {"changed": false, "name": "usb-storage", "params": "", "state": "absent"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.2.1 Ensure package manager repositories are configured] ***
ok: [172.20.0.4] => {
   "msg": "Run the following command and verify package repositories are configured correctly\n>
apt-cache policy\nRemediation:\nConfigure your package manager repositories according to site
policy\n"
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.2.2 Ensure GPG keys are configured] *********
ok: [172.20.0.4] => {
   "msg": "Audit:\nVerify GPG keys are configured correctly for your package manager:\n> apt-key
list\nRemediation:\nUpdate your package manager GPG keys in accordance with site policy.\n"
}

TASK [CIS-Ubuntu-20.04-Ansible : 1.3.1 Ensure sudo is installed] ***************
ok: [172.20.0.4] => {"cache_update_time": 1698270825, "cache_updated": false, "changed": false}

TASK [CIS-Ubuntu-20.04-Ansible : 1.3.2 Ensure sudo commands use pty] ***********
```

```
changed: [172.20.0.4] => {"backup": "", "changed": true, "msg": "line added"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.3.3 Ensure sudo log file exists] ************
changed: [172.20.0.4] => {"backup": "", "changed": true, "msg": "line added"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.3.1 Ensure AIDE is installed] ***************
changed: [172.20.0.4] => {"cache_update_time": 1698270825, "cache_updated": false, "changed": true, "stderr": "Can't exec \"/tmp/ssl-cert.config.mBH9HZ\": Permission denied at /usr/share/perl/5.30/IPC/Open3.pm line 281.\nopen2: exec of /tmp/ssl-cert.config.mBH9HZ configure failed: Permission denied at /usr/share/perl5/Debconf/ConfModule.pm line 59.\n", "stderr_lines": ["Can't exec \"/tmp/ssl-cert.config.mBH9HZ\": Permission denied at /usr/share/perl/5.30/IPC/Open3.pm line 281.", "open2: exec of /tmp/ssl-cert.config.mBH9HZ configure failed: Permission denied at /usr/share/perl5/Debconf/ConfModule.pm line 59."], "stdout": "Reading package lists...\nBuilding dependency tree...\nReading state information...\nThe following additional packages will be installed:\n  bsd-mailx liblockfile-bin liblockfile1 postfix ssl-cert\nSuggested packages:\n  figlet procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre\n  postfix-lmdb postfix-sqlite sasl2-bin | dovecot-common resolvconf\n  postfix-cdb postfix-doc openssl-blacklist\nThe following NEW packages will be installed:\n  aide aide-common bsd-mailx liblockfile-bin liblockfile1 postfix ssl-cert\n0 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.\nNeed to get 2135 kB of archives.\nAfter this operation, 7494 kB of additional disk space will be used.\nGet:1 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal-updates/main amd64 aide amd64 0.16.1-1ubuntu0.1 [765 kB]\nGet:2 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal/main amd64 ssl-cert all 1.0.39 [17.0 kB]\nGet:3 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal-updates/main amd64 postfix amd64 3.4.13-0ubuntu1.2 [1201 kB]\nGet:4 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal/main amd64 liblockfile-bin amd64 1.16-1.1 [11.7 kB]\nGet:5 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal/main amd64 liblockfile1 amd64 1.16-1.1 [6680 B]\nGet:6 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal/main amd64 bsd-mailx amd64 8.1.2-0.20180807cvs-1 [67.2 kB]\nGet:7 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal-updates/main amd64 aide-common all 0.16.1-1ubuntu0.1 [66.4 kB]\nPreconfiguring packages ...\nFetched 2135 kB in 0s (29.1 MB/s)\nSelecting previously unselected package aide.\r\n(Reading database ... \r(Reading database ... 5%\r(Reading database ... 10%\r(Reading database ... 15%\r(Reading database ... 20%\r(Reading database ... 25%\r(Reading database ... 30%\r(Reading database ... 35%\r(Reading database ... 40%\r(Reading database ... 45%\r(Reading database ... 50%\r(Reading database ... 55%\r(Reading database ... 60%\r(Reading database ... 65%\r(Reading database ... 70%\r(Reading database ... 75%\r(Reading database ... 80%\r(Reading database ... 85%\r(Reading database ... 90%\r(Reading database ... 95%\r(Reading database ... 100%\r(Reading database ... 62002 files and directories currently installed.)\r\nPreparing to unpack .../0-aide_0.16.1-1ubuntu0.1_amd64.deb ...\r\nUnpacking aide (0.16.1-1ubuntu0.1) ...\r\nSelecting previously unselected package ssl-cert.\r\nPreparing to unpack .../1-ssl-cert_1.0.39_all.deb ...\r\nUnpacking ssl-cert (1.0.39) ...\r\nSelecting previously unselected package postfix.\r\nPreparing to unpack .../2-postfix_3.4.13-0ubuntu1.2_amd64.deb ...\r\nUnpacking postfix (3.4.13-0ubuntu1.2) ...\r\nSelecting previously unselected package liblockfile-bin.\r\nPreparing to unpack .../3-liblockfile-bin_1.16-1.1_amd64.deb ...\r\nUnpacking liblockfile-bin (1.16-1.1) ...\r\nSelecting previously unselected package liblockfile1:amd64.\r\nPreparing to unpack .../4-liblockfile1_1.16-1.1_amd64.deb ...\r\nUnpacking liblockfile1:amd64 (1.16-1.1) ...\r\nSelecting previously unselected package bsd-mailx.\r\nPreparing to unpack .../5-bsd-mailx_8.1.2-0.20180807cvs-1_amd64.deb ...\r\nUnpacking bsd-mailx (8.1.2-0.20180807cvs-1) ...\r\nSelecting previously unselected package aide-common.\r\nPreparing to unpack .../6-aide-common_0.16.1-1ubuntu0.1_all.deb ...\r\nUnpacking aide-common (0.16.1-1ubuntu0.1) ...\r\nSetting up aide (0.16.1-1ubuntu0.1) ...\r\nSetting up liblockfile-bin (1.16-1.1) ...\r\nSetting up ssl-cert (1.0.39) ...\r\nSetting up postfix (3.4.13-0ubuntu1.2) ...\r\nAdding group `postfix' (GID 121) ...\r\nDone.\r\nAdding system user `postfix' (UID 114) ...\r\nAdding new user `postfix' (UID 114) with group `postfix' ...\r\nNot creating home directory `/var/spool/postfix'.\r\nCreating /etc/postfix/dynamicmaps.cf\r\nAdding group `postdrop' (GID 122) ...\r\nDone.\r\nsetting myhostname: ip-172-31-32-140.eu-west-2.compute.internal\r\nsetting alias maps\r\nsetting alias database\r\nchanging /etc/mailname to ip-172-31-32-140.eu-west-2.compute.internal\r\nsetting myorigin\r\nsetting destinations: $myhostname, ip-172-31-32-140.eu-west-2.compute.internal, localhost.eu-west-2.compute.internal, , localhost\r\nsetting relayhost: \r\nsetting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128\r\nsetting mailbox_size_limit: 0\r\nsetting recipient_delimiter: +\r\nsetting inet_interfaces: all\r\nsetting inet_protocols: all\r\n/etc/aliases does not exist, creating it.\r\nWARNING: /etc/aliases exists, but does not have a root alias.\r\n\r\nPostfix (main.cf) is now set up with a default configuration.  If you need to \r\nmake changes, edit /etc/postfix/main.cf (and others) as needed.  To view \r\nPostfix configuration values, see
```

postconf(1).\r\n\r\nAfter modifying main.cf, be sure to run 'systemctl reload postfix'.\r\n\r\nRunning newaliases\r\nCreated symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /lib/systemd/system/postfix.service.\r\nSetting up liblockfile1:amd64 (1.16-1.1) ...\r\nSetting up bsd-mailx (8.1.2-0.20180807cvs-1) ...\r\nupdate-alternatives: using /usr/bin/bsd-mailx to provide /usr/bin/mailx (mailx) in auto mode\r\nSetting up aide-common (0.16.1-1ubuntu0.1) ...\r\n\r\nCreating config file /etc/cron.daily/aide with new version\r\n\r\nCreating config file /etc/default/aide with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_adjtime with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_util-linux with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_munin-nodes with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_proftpd with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_tetex-bin with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_slrn with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_acpid with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_opie-server with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_aide with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_initramfs-tools with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_dovecot with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_nagios2 with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_cron-apt with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_openvpn with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_apache2 with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_nagios3 with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_clamav with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_systemd_journal with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_privoxy with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_isc-dhcp-client with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_ssh-server with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_amavisd-new with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_postgresql with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_lastlog with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_xfree86-common with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/70_aide_run with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_mlocate with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_wtmp with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_isc-dhcp-server with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/10_aide_constants with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_apt with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_btmp with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_initscripts with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_logrotate with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_ifplugd with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_cereal with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_dokuwiki with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_exim4_logs with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_mdadm with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_rsyslog with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/10_aide_run with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_spamassassin with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_debsecan with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_cron with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_findutils with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_rkhunter with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_ddclient with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_resolvconf with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_boinc-client with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_apt-listbugs with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_nslcd with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_cracklib-runtime with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_exim4 with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/99_aide_root with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_nfs with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_gnupg with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_screen with new version\r\n\r\nCreating config file

```
/etc/aide/aide.conf.d/31_aide_lib-init-rw with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_sudo with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/70_aide_dev with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/30_inn2_vars with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_cups with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_root-dotfiles with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/30_aide_apache2 with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_samba with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_at with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_tiger with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/70_aide_etc with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_dlocate with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_x11-common with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_fcron with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_run_systemd_netif with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_pm-utils with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_x11-xkb-utils with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_slapd with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_xdm with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_pcscd with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_apt-listchanges with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/70_aide_proc_sys with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_etckeeper with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_torrus with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_apcupsd with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_postfix with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_php7 with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_dbus with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_vpnc with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_anubis with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_apt-show-versions with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_apt_frqchg with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_libvirt-bin with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_laptop-mode-tools with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_console-log with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/10_aide_year with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_squid with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_systemd_sessions with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_checksecurity with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_snmpd with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_lvm2 with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_runuser with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_svn-server with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_atop with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_mysql-server with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_modules with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_bind9 with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_mailman with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_rngd with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_kerberos with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/10_aide_distribution with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/30_aide_bind9 with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_aptitude with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_smokeping with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_man with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_apt-file with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_inetd with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_apache with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_libapache2-mod-fastcgi with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_rsnapshot with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_anacron with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/10_aide_prevyear with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_inn2 with new version\r\n\r\nCreating config file
/etc/aide/aide.conf.d/31_aide_ifupdown with new version\r\n\r\nCreating config file
```

/etc/aide/aide.conf.d/31_aide_run_systemd_resolve with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_mail with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_hald with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_ippl with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/10_aide_hostname with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_trac with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_amanda-server with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_debconf with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_xinetd with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_network with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_udev with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_nscd with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/70_aide_tmp with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_mtab with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_lighttpd with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/70_aide_var with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_aptitude_frqchg with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_php-common with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_ntp-server with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_amanda-client with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_crack with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_webalizer with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_clamav-freshclam with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_utmp with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_smartmontools with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_ssh-agent with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_portmap with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_postgrey with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_pam_motd with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_dpkg with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_alsa with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_wpasupplicant with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_logcheck with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_hapsd with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_nrpe with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_tt-rss with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_munin with new version\r\n\r\nCreating config file /etc/aide/aide.conf.d/31_aide_fail2ban with new version\r\n\r\nCreating config file /etc/aide/aide.settings.d/10_aide_sourceslist with new version\r\n\r\nCreating config file /etc/aide/aide.settings.d/31_aide_trac_settings with new version\r\n\r\nCreating config file /etc/aide/aide.settings.d/31_aide_svn-server_settings with new version\r\n\r\nCreating config file /etc/aide/aide.settings.d/31_aide_apt_settings with new version\r\n\r\nCreating config file /etc/aide/aide.conf with new version\r\nProcessing triggers for rsyslog (8.2001.0-1ubuntu1.3) ...\r\nProcessing triggers for ufw (0.36-6ubuntu1.1) ...\r\nProcessing triggers for systemd (245.4-4ubuntu3.22) ...\r\nProcessing triggers for man-db (2.9.1-1) ...\r\nProcessing triggers for libc-bin (2.31-0ubuntu9.12) ...\r\n", "stdout_lines": ["Reading package lists...", "Building dependency tree...", "Reading state information...", "The following additional packages will be installed:", " bsd-mailx liblockfile-bin liblockfile1 postfix ssl-cert", "Suggested packages:", " figlet procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre", " postfix-lmdb postfix-sqlite sasl2-bin | dovecot-common resolvconf", " postfix-cdb postfix-doc openssl-blacklist", "The following NEW packages will be installed:", " aide aide-common bsd-mailx liblockfile-bin liblockfile1 postfix ssl-cert", "0 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.", "Need to get 2135 kB of archives.", "After this operation, 7494 kB of additional disk space will be used.", "Get:1 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal-updates/main amd64 aide amd64 0.16.1-1ubuntu0.1 [765 kB]", "Get:2 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal/main amd64 ssl-cert all 1.0.39 [17.0 kB]", "Get:3 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal-updates/main amd64 postfix amd64 3.4.13-0ubuntu1.2 [1201 kB]", "Get:4 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal/main amd64 liblockfile-bin amd64 1.16-1.1 [11.7 kB]", "Get:5 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal/main amd64 liblockfile1 amd64 1.16-1.1 [6680 B]", "Get:6 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal/main amd64 bsd-mailx amd64 8.1.2-0.20180807cvs-1 [67.2 kB]", "Get:7 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu focal-updates/main amd64 aide-common all 0.16.1-1ubuntu0.1 [66.4 kB]", "Preconfiguring packages ...", "Fetched 2135 kB in 0s (29.1 MB/s)", "Selecting previously unselected package aide.", "(Reading database ... ", "(Reading

database ... 5%", "(Reading database ... 10%", "(Reading database ... 15%", "(Reading database ... 20%", "(Reading database ... 25%", "(Reading database ... 30%", "(Reading database ... 35%", "(Reading database ... 40%", "(Reading database ... 45%", "(Reading database ... 50%", "(Reading database ... 55%", "(Reading database ... 60%", "(Reading database ... 65%", "(Reading database ... 70%", "(Reading database ... 75%", "(Reading database ... 80%", "(Reading database ... 85%", "(Reading database ... 90%", "(Reading database ... 95%", "(Reading database ... 100%", "(Reading database ... 62002 files and directories currently installed.)", "Preparing to unpack .../0-aide_0.16.1-1ubuntu0.1_amd64.deb ...", "Unpacking aide (0.16.1-1ubuntu0.1) ...", "Selecting previously unselected package ssl-cert.", "Preparing to unpack .../1-ssl-cert_1.0.39_all.deb ...", "Unpacking ssl-cert (1.0.39) ...", "Selecting previously unselected package postfix.", "Preparing to unpack .../2-postfix_3.4.13-0ubuntu1.2_amd64.deb ...", "Unpacking postfix (3.4.13-0ubuntu1.2) ...", "Selecting previously unselected package liblockfile-bin.", "Preparing to unpack .../3-liblockfile-bin_1.16-1.1_amd64.deb ...", "Unpacking liblockfile-bin (1.16-1.1) ...", "Selecting previously unselected package liblockfile1:amd64.", "Preparing to unpack .../4-liblockfile1_1.16-1.1_amd64.deb ...", "Unpacking liblockfile1:amd64 (1.16-1.1) ...", "Selecting previously unselected package bsd-mailx.", "Preparing to unpack .../5-bsd-mailx_8.1.2-0.20180807cvs-1_amd64.deb ...", "Unpacking bsd-mailx (8.1.2-0.20180807cvs-1) ...", "Selecting previously unselected package aide-common.", "Preparing to unpack .../6-aide-common_0.16.1-1ubuntu0.1_all.deb ...", "Unpacking aide-common (0.16.1-1ubuntu0.1) ...", "Setting up aide (0.16.1-1ubuntu0.1) ...", "Setting up liblockfile-bin (1.16-1.1) ...", "Setting up ssl-cert (1.0.39) ...", "Setting up postfix (3.4.13-0ubuntu1.2) ...", "Adding group `postfix' (GID 121) ...", "Done.", "Adding system user `postfix' (UID 114) ...", "Adding new user `postfix' (UID 114) with group `postfix' ...", "Not creating home directory `/var/spool/postfix'.", "Creating /etc/postfix/dynamicmaps.cf", "Adding group `postdrop' (GID 122) ...", "Done.", "setting myhostname: ip-172-31-32-140.eu-west-2.compute.internal", "setting alias maps", "setting alias database", "changing /etc/mailname to ip-172-31-32-140.eu-west-2.compute.internal", "setting myorigin", "setting destinations: $myhostname, ip-172-31-32-140.eu-west-2.compute.internal, localhost.eu-west-2.compute.internal, , localhost", "setting relayhost: ", "setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128", "setting mailbox_size_limit: 0", "setting recipient_delimiter: +", "setting inet_interfaces: all", "setting inet_protocols: all", "/etc/aliases does not exist, creating it.", "WARNING: /etc/aliases exists, but does not have a root alias.", "", "Postfix (main.cf) is now set up with a default configuration. If you need to ", "make changes, edit /etc/postfix/main.cf (and others) as needed. To view ", "Postfix configuration values, see postconf(1).", "", "After modifying main.cf, be sure to run 'systemctl reload postfix'.", "", "Running newaliases", "Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /lib/systemd/system/postfix.service.", "Setting up liblockfile1:amd64 (1.16-1.1) ...", "Setting up bsd-mailx (8.1.2-0.20180807cvs-1) ...", "update-alternatives: using /usr/bin/bsd-mailx to provide /usr/bin/mailx (mailx) in auto mode", "Setting up aide-common (0.16.1-1ubuntu0.1) ...", "", "Creating config file /etc/cron.daily/aide with new version", "", "Creating config file /etc/default/aide with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_adjtime with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_util-linux with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_munin-nodes with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_proftpd with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_tetex-bin with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_slrn with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_acpid with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_opie-server with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_aide with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_initramfs-tools with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_dovecot with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_nagios2 with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_cron-apt with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_openvpn with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_apache2 with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_nagios3 with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_clamav with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_systemd_journal with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_privoxy with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_isc-dhcp-client with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_ssh-server with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_amavisd-new with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_postgresql with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_lastlog with new version", "", "Creating config file

```
/etc/aide/aide.conf.d/31_aide_xfree86-common with new version", "", "Creating config file
/etc/aide/aide.conf.d/70_aide_run with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_mlocate with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_wtmp with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_isc-dhcp-server with new version", "", "Creating config file
/etc/aide/aide.conf.d/10_aide_constants with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_apt with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_btmp with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_initscripts with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_logrotate with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_ifplugd with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_cereal with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_dokuwiki with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_exim4_logs with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_mdadm with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_rsyslog with new version", "", "Creating config file
/etc/aide/aide.conf.d/10_aide_run with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_spamassassin with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_debsecan with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_cron with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_findutils with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_rkhunter with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_ddclient with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_resolvconf with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_boinc-client with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_apt-listbugs with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_nslcd with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_cracklib-runtime with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_exim4 with new version", "", "Creating config file
/etc/aide/aide.conf.d/99_aide_root with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_nfs with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_gnupg with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_screen with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_lib-init-rw with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_sudo with new version", "", "Creating config file
/etc/aide/aide.conf.d/70_aide_dev with new version", "", "Creating config file
/etc/aide/aide.conf.d/30_inn2_vars with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_cups with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_root-dotfiles with new version", "", "Creating config file
/etc/aide/aide.conf.d/30_aide_apache2 with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_samba with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_at with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_tiger with new version", "", "Creating config file
/etc/aide/aide.conf.d/70_aide_etc with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_dlocate with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_x11-common with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_fcron with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_run_systemd_netif with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_pm-utils with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_x11-xkb-utils with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_slapd with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_xdm with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_pcscd with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_apt-listchanges with new version", "", "Creating config file
/etc/aide/aide.conf.d/70_aide_proc_sys with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_etckeeper with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_torrus with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_apcupsd with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_postfix with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_php7 with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_dbus with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_vpnc with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_anubis with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_apt-show-versions with new version", "", "Creating config file
```

```
/etc/aide/aide.conf.d/31_aide_apt_frqchg with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_libvirt-bin with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_laptop-mode-tools with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_console-log with new version", "", "Creating config file
/etc/aide/aide.conf.d/10_aide_year with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_squid with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_systemd_sessions with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_checksecurity with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_snmpd with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_lvm2 with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_runuser with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_svn-server with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_atop with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_mysql-server with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_modules with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_bind9 with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_mailman with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_rngd with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_kerberos with new version", "", "Creating config file
/etc/aide/aide.conf.d/10_aide_distribution with new version", "", "Creating config file
/etc/aide/aide.conf.d/30_aide_bind9 with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_aptitude with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_smokeping with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_man with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_apt-file with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_inetd with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_apache with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_libapache2-mod-fastcgi with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_rsnapshot with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_anacron with new version", "", "Creating config file
/etc/aide/aide.conf.d/10_aide_prevyear with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_inn2 with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_ifupdown with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_run_systemd_resolve with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_mail with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_hald with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_ippl with new version", "", "Creating config file
/etc/aide/aide.conf.d/10_aide_hostname with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_trac with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_amanda-server with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_debconf with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_xinetd with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_network with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_udev with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_nscd with new version", "", "Creating config file
/etc/aide/aide.conf.d/70_aide_tmp with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_mtab with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_lighttpd with new version", "", "Creating config file
/etc/aide/aide.conf.d/70_aide_var with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_aptitude_frqchg with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_php-common with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_ntp-server with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_amanda-client with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_crack with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_webalizer with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_clamav-freshclam with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_utmp with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_smartmontools with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_ssh-agent with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_portmap with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_postgrey with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_pam_motd with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_dpkg with new version", "", "Creating config file
/etc/aide/aide.conf.d/31_aide_alsa with new version", "", "Creating config file
```

/etc/aide/aide.conf.d/31_aide_wpasupplicant with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_logcheck with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_hapsd with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_nrpe with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_tt-rss with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_munin with new version", "", "Creating config file /etc/aide/aide.conf.d/31_aide_fail2ban with new version", "", "Creating config file /etc/aide/aide.settings.d/10_aide_sourceslist with new version", "", "Creating config file /etc/aide/aide.settings.d/31_aide_trac_settings with new version", "", "Creating config file /etc/aide/aide.settings.d/31_aide_svn-server_settings with new version", "", "Creating config file /etc/aide/aide.settings.d/31_aide_apt_settings with new version", "", "Creating config file /etc/aide/aide.conf with new version", "Processing triggers for rsyslog (8.2001.0-1ubuntu1.3) ...", "Processing triggers for ufw (0.36-6ubuntu1.1) ...", "Processing triggers for systemd (245.4-4ubuntu3.22) ...", "Processing triggers for man-db (2.9.1-1) ...", "Processing triggers for libc-bin (2.31-0ubuntu9.12) ..."]}

TASK [CIS-Ubuntu-20.04-Ansible : Configure default AIDE excludes file] *********

changed: [172.20.0.4] => {"changed": true, "checksum": "70d8669a74ec2e060b7e180a738aa7efcb594546", "dest": "/etc/aide/aide.conf.d/00_local_excludes", "gid": 0, "group": "root", "md5sum": "7a332f6ff06e4a53342fa05cc26f224d", "mode": "0644", "owner": "root", "size": 677, "src": "/home/ubuntu/.ansible/tmp/ansible-tmp-1702137971.066711-35773-151274905262378/source", "state": "file", "uid": 0}

TASK [CIS-Ubuntu-20.04-Ansible : Simplify AIDE checksums] **********

skipping: [172.20.0.4] => {"changed": false, "skip_reason": "Conditional result was False"}

TASK [CIS-Ubuntu-20.04-Ansible : Add extra AIDE exclude paths] *****

skipping: [172.20.0.4] => {"changed": false, "skip_reason": "Conditional result was False"}

TASK [CIS-Ubuntu-20.04-Ansible : Configure AIDE as appropriate for your environment | aideinit] ***

changed: [172.20.0.4] => {"changed": true, "cmd": ["aideinit", "--yes", "--force"], "delta": "0:08:04.722876", "end": "2023-12-09 16:14:20.665055", "msg": "", "rc": 0, "start": "2023-12-09 16:06:15.942179", "stderr": "Running aide --init...", "stderr_lines": ["Running aide --init..."], "stdout": "Start timestamp: 2023-12-09 16:06:18 +0000 (AIDE 0.16.1)\nAIDE initialized database at /var/lib/aide/aide.db.new\nVerbose level: 6\n\nNumber of entries:\t97312\n\n---------------------------------\nThe attributes of the (uncompressed) database(s):\n--\n\n/var/lib/aide/aide.db.new\n RMD160 : 85ia8dD10ioO3C2By4BACcihwsc=\n TIGER : Bna5nyPWLEmXvclqiJmPXhT3rgNRq+tx\n SHA256 : A60tHVXlDYdnseXCPLSvKQsBdMB1XPWN\n cIB/r6YfQP0=\n SHA512 : YEOvZfmXTXZ7JjkbLZb3TsLuZIUg+bpT\n ukKl84XMsMnjY6oj9xUV3lT8NltlS8jF\n Y/I2SblcKu1WSf3p5kVNYw==\n CRC32 : ZDuyvg==\n HAVAL : uJsy3zAgwIIzwImNYsXybW9/Fc0coD3q\n aTPgBV3dbHU=\n GOST : aAfcPz4NUojKwAZaUrrQEsiFxy7swHWi\n tnAC487v0M8=\n\n\nEnd timestamp: 2023-12-09 16:14:20 +0000 (run time: 8m 2s)", "stdout_lines": ["Start timestamp: 2023-12-09 16:06:18 +0000 (AIDE 0.16.1)", "AIDE initialized database at /var/lib/aide/aide.db.new", "Verbose level: 6", "", "Number of entries:\t97312", "", "---------------------------------", "The attributes of the (uncompressed) database(s):", "--", "", "/var/lib/aide/aide.db.new", " RMD160 : 85ia8dD10ioO3C2By4BACcihwsc=", " TIGER : Bna5nyPWLEmXvclqiJmPXhT3rgNRq+tx", " SHA256 : A60tHVXlDYdnseXCPLSvKQsBdMB1XPWN", " cIB/r6YfQP0=", " SHA512 : YEOvZfmXTXZ7JjkbLZb3TsLuZIUg+bpT", " ukKl84XMsMnjY6oj9xUV3lT8NltlS8jF", " Y/I2SblcKu1WSf3p5kVNYw==", " CRC32 : ZDuyvg==", " HAVAL : uJsy3zAgwIIzwImNYsXybW9/Fc0coD3q", " aTPgBV3dbHU=", " GOST : aAfcPz4NUojKwAZaUrrQEsiFxy7swHWi", " tnAC487v0M8=", "", "", "End timestamp: 2023-12-09 16:14:20 +0000 (run time: 8m 2s)"]}

TASK [CIS-Ubuntu-20.04-Ansible : Configure AIDE as appropriate for your environment | aideinit db] ***

changed: [172.20.0.4] => {"changed": true, "cmd": "mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db\n", "delta": "0:00:00.094816", "end": "2023-12-09 16:14:24.215068", "msg": "", "rc": 0, "start": "2023-12-09 16:14:24.120252", "stderr": "", "stderr_lines": [], "stdout": "", "stdout_lines": []}

TASK [CIS-Ubuntu-20.04-Ansible : 1.3.2 Ensure filesystem integrity is regularly checked | Cron] ***

changed: [172.20.0.4] => {"changed": true, "envs": [], "jobs": ["Run AIDE integrity check weekly"]}

```
TASK [CIS-Ubuntu-20.04-Ansible : 1.4.2 Ensure bootloader password is set - step 1 - check
bootloader_credentials.password has been changed] ***
skipping: [172.20.0.4] => {"changed": false, "skip_reason": "Conditional result was False"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.4.2 Ensure bootloader password is set - step 2 - check if it
isn't already set up] ***
skipping: [172] => {"changed": false, "skip_reason": "Conditional result was False"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.4.2 Ensure bootloader password is set - step 3 - create
bootloader password hash] ***
skipping: [172.20.0.4] => {"changed": false, "skip_reason": "Conditional result was False"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.4.2 Ensure bootloader password is set - step 4 - create custom
grub configuration file] ***
skipping: [172.20.0.4] => {"changed": false, "skip_reason": "Conditional result was False"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.4.2 Ensure bootloader password is set - step 4 - update grub]
***
skipping: [172.20.0.4] => {"changed": false, "skip_reason": "Conditional result was False"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.4.3 Ensure permissions on bootloader config are configured]
***
changed: [172.20.0.4] => {"changed": true, "gid": 0, "group": "root", "mode": "0400", "owner":
"root", "path": "/boot/grub/grub.cfg", "size": 8176, "state": "file", "uid": 0}

TASK [CIS-Ubuntu-20.04-Ansible : 1.4.4 Ensure authentication required for single user mode -
check root_password has been changed] ***
fatal: [172.20.0.4]: FAILED! => {"changed": false, "msg": "Exiting: Change root_password from
r00tP4ssw0rd in defaults/main.yml"}

TASK [CIS-Ubuntu-20.04-Ansible : 1.4.4 Ensure authentication required for single user mode -
create a root password] ***
fatal: [172.20.0.4]: FAILED! => {"msg": "crypt.crypt not supported on Mac OS X/Darwin, install
passlib python module. crypt.crypt not supported on Mac OS X/Darwin, install passlib python
module"}

PLAY RECAP *********************************************************************
172.20.0.4                 : ok=45   changed=19   unreachable=0    failed=1    skipped=10   rescued=1
ignored=2
```

Додаток Г

Набір інструкцій у файлі tasks/section_4_Logging_and_Auditing

```
---
# 4 Logging and Auditing
# 4.1 Configure System Accounting (auditd)
# 4.1.1 Ensure auditing is enabled
# 4.1.1.1 Ensure auditd is installed
# The capturing of system events provides system administrators with information to allow them to
determine if unauthorized access to their system is occurring.
- name: 4.1.1.1 Ensure auditd is installed
 apt:
   name: ["auditd", "audispd-plugins"]
   state: present
   install_recommends: false
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.1.1
# 4.1.1.2 Ensure auditd service is enabled
# The capturing of system events provides system administrators with information to allow them to
determine if unauthorized access to their system is occurring.
- name: 4.1.1.2 Ensure auditd service is enabled
 service:
   name: auditd
   state: started
   enabled: true
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.1.2
# 4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled
- name: 4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled
 # Audit events need to be captured on processes that start up prior to auditd , so that potential
malicious activity cannot go undetected.
 replace:
   dest: /etc/default/grub
   regexp: '^(GRUB_CMDLINE_LINUX=(?!.*audit)\"[^\"]*)(\".*)'
   replace: '\1 audit=1\2'
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.1.3
# 4.1.1.4 Ensure audit_backlog_limit is sufficient
# during boot if audit=1, then the backlog will hold 64 records. If more that 64 records are created
during boot, auditd records will be lost and potential malicious activity could go undetected.
- name: 4.1.1.4 Ensure audit_backlog_limit is sufficient
 replace:
   dest: /etc/default/grub
   regexp: '^(GRUB_CMDLINE_LINUX=(?!.*audit_backlog_limit)\"[^\"]*)(\".*)'
   replace: '\1 audit_backlog_limit={{grub_backlog_limit}}\2'
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.1.4
# 4.1.2 Configure Data Retention
# 4.1.2.1 Ensure audit log storage size is configured
- name: 4.1.2.1 Ensure audit log storage size is configured
 lineinfile:
   dest: /etc/audit/auditd.conf
   regexp: "^max_log_file( |=)"
   line: "max_log_file = {{ max_log_file }}"
```

```
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.2.1
# 4.1.2.2 Ensure audit logs are not automatically deleted
- name: 4.1.2.2 Ensure audit logs are not automatically deleted
 lineinfile:
   dest: /etc/audit/auditd.conf
   regexp: "^max_log_file_action"
   line: "max_log_file_action = {{ max_log_file_action }}"
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.2.2
# 4.1.2.3 Ensure system is disabled when audit logs are full
- name: 4.1.2.3 Ensure system is disabled when audit logs are full
 block:
   - name: 4.1.2.3 Ensure system is disabled when audit logs are full | admin_space_left_action
     lineinfile:
       dest: /etc/audit/auditd.conf
       regexp: "^admin_space_left_action"
       line: "admin_space_left_action = {{ admin_space_left_action }}"
   - name: 4.1.2.3 Ensure system is disabled when audit logs are full | space_left_action
     lineinfile:
       dest: /etc/audit/auditd.conf
       regexp: "^space_left_action"
       line: "space_left_action = {{ space_left_action }}"
   - name: 4.1.2.3 Ensure system is disabled when audit logs are full | action_mail_acct
     lineinfile:
       dest: /etc/audit/auditd.conf
       regexp: "^action_mail_acct"
       line: "action_mail_acct = {{ action_mail_acct }}"
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.2.3
# 4.1.3 Ensure events that modify date and time information are collected
# Unexpected changes in system date and/or time could be a sign of malicious activity on the system.
- name: 4.1.3 Ensure events that modify date and time information are collected
 template:
   src: files/templates/auditd/time-change.rules.j2
   dest: /etc/audit/rules.d/time-change.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.3
# 4.1.4 Ensure events that modify user/group information are collected
# # Unexpected changes to these files could be an indication that the system has been compromised and
that an unauthorized user is attempting to hide their activities or compromise additional accounts.
- name: 4.1.4 Ensure events that modify user/group information are collected
 template:
   src: files/templates/auditd/identity.rules.j2
   dest: /etc/audit/rules.d/identity.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.4
```

```
# 4.1.5 Ensure events that modify the system's network environment are collected
# Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and
domainname of a system. The changing of these names could potentially break
# security parameters that are set based on those names. The /etc/hosts file is monitored for changes
in the file that can indicate an unauthorized intruder is trying to change
# machine associations with IP addresses and trick users and processes into connecting to unintended
machines. Monitoring /etc/issue and /etc/issue.net is important, as
# intruders could put disinformation into those files and trick users into providing information to the
intruder. Monitoring /etc/network is important as it can show if
# network interfaces or scripts are being modified in a way that can lead to the machine becoming
unavailable or compromised. All audit records will be tagged with the identifier "system-locale."
- name: 4.1.5 Ensure events that modify the system's network environment are collected
 template:
   src: files/templates/auditd/system-locale.rules.j2
   dest: /etc/audit/rules.d/system-locale.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.5
# 4.1.6 Ensure events that modify the system's Mandatory Access Controls are collected
# # Changes to files in these directories could indicate that an unauthorized user is attempting to
modify access controls and change security contexts, leading to a compromise of the system.
- name: 4.1.6 Ensure events that modify the system's Mandatory Access Controls are collected
 template:
   src: files/templates/auditd/MAC-policy.rules.j2
   dest: /etc/audit/rules.d/MAC-policy.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.6
# 4.1.7 Ensure login and logout events are collected
# Monitoring login/logout events could provide a system administrator with information associated with
brute force attacks against user logins.
- name: 4.1.7 Ensure login and logout events are collected
 template:
   src: files/templates/auditd/logins.rules.j2
   dest: /etc/audit/rules.d/logins.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.7
# 4.1.8 Ensure session initiation information is collected
# # Monitoring these files for changes could alert a system administrator to logins occurring at
unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do
not normally log in).
- name: 4.1.8 Ensure session initiation information is collected
 template:
   src: files/templates/auditd/session.rules.j2
   dest: /etc/audit/rules.d/session.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
```

```
   - 4.1.8
# 4.1.9 Ensure discretionary access control permission modification events are collected
# Monitoring for changes in file attributes could alert a system administrator to activity that could
indicate intruder activity or policy violation.
- name: 4.1.9 Ensure discretionary access control permission modification events are collected
 template:
   src: files/templates/auditd/perm_mod.rules.j2
   dest: /etc/audit/rules.d/perm_mod.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.9
# 4.1.10 Ensure unsuccessful unauthorized file access attempts are collected
# Failed attempts to open, create or truncate files could be an indication that an individual or
process is trying to gain unauthorized access to the system.
- name: 4.1.10 Ensure unsuccessful unauthorized file access attempts are collected
 template:
   src: files/templates/auditd/audit.rules.j2
   dest: /etc/audit/rules.d/audit.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.10
# 4.1.11 Ensure use of privileged commands is collected
- name: 4.1.11 Ensure use of privileged commands is collected
 block:
   - name: 4.1.11 Ensure use of privileged commands is collected | get data
     script: 4_1_11.sh
     register: output_4_1_11
   - name: 4.1.11 Ensure use of privileged commands is collected | apply
     template:
       src: files/templates/auditd/privileged.rules.j2
       dest: /etc/audit/rules.d/privileged.rules
       owner: root
       group: root
       mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.11
# 4.1.12 Ensure successful file system mounts are collected
# It is highly unusual for a non privileged user to mount file systems to the system. While tracking
mount commands gives the system administrator evidence that external media
# may have been mounted (based on a review of the source of the mount and confirming it's an external
media type), it does not conclusively indicate that data was exported to the
# media. System administrators who wish to determine if data were exported, would also have to track
successful open , creat and truncate system calls requiring write access to a
# file under the mount point of the external media file system. This could give a fair indication that
a write occurred. The only way to truly prove it, would be to track
# successful writes to the external media. Tracking write system calls could quickly fill up the audit
log and is not recommended. Recommendations on configuration options to track data export to media is
beyond the scope of this document.
- name: 4.1.12 Ensure successful file system mounts are collected
 template:
   src: files/templates/auditd/system_mounts.rules.j2
   dest: /etc/audit/rules.d/system_mounts.rules
   owner: root
   group: root
   mode: 0600
```

```
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.12
# 4.1.13 Ensure file deletion events by users are collected
# Monitoring these calls from non-privileged users could provide a system administrator with evidence
that inappropriate removal of files and file attributes associated with
# protected files is occurring. While this audit option will look at all events, system administrators
will want to look for specific privileged files that are being deleted or altered.
- name: 4.1.13 Ensure file deletion events by users are collected
 template:
   src: files/templates/auditd/delete.rules.j2
   dest: /etc/audit/rules.d/delete.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.13
# 4.1.14 Ensure changes to system administration scope (sudoers) is collected
# Changes in the /etc/sudoers file can indicate that an unauthorized change has been made to scope of
system administrator activity.
- name: 4.1.14 Ensure changes to system administration scope (sudoers) is collected
 template:
   src: files/templates/auditd/scope.rules.j2
   dest: /etc/audit/rules.d/scope.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.14
# 4.1.15 Ensure system administrator command executions (sudo) are collected
# # # Creating an audit log of administrators with temporary elevated privileges and the operation(s)
they performed is essential to reporting. Administrators will want to correlate the events written to
the audit trail with the records written to sudo logfile to verify if unauthorized commands have been
executed.
- name: 4.1.15 Ensure system administrator command executions (sudo) are collected
 template:
   src: files/templates/auditd/actions.rules.j2
   dest: /etc/audit/rules.d/actions.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.15
# 4.1.16 Ensure kernel module loading and unloading is collected
# # # # Monitoring the use of insmod , rmmod and modprobe could provide system administrators with
evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the
security of the system. Monitoring of the init_module and delete_module system calls would reflect an
unauthorized user attempting to use a different program to load and unload modules.
- name: 4.1.16 Ensure kernel module loading and unloading is collected
 template:
   src: files/templates/auditd/modules.rules.j2
   dest: /etc/audit/rules.d/modules.rules
   owner: root
   group: root
   mode: 0600
 tags:
   - section4
```

```
   - level_2_server
   - level_2_workstation
   - 4.1.16
# 4.1.17 Ensure the audit configuration is immutable
# # # In immutable mode, unauthorized users cannot execute changes to the audit system to potentially
hide malicious activity and then put the audit rules back. Users would most likely notice a system
reboot and that could alert administrators of an attempt to make unauthorized audit changes.
- name: 4.1.17 Ensure the audit configuration is immutable
 block:
   - name: 4.1.17 Ensure the audit configuration is immutable
     template:
       src: files/templates/auditd/99-finalize.rules.j2
       dest: /etc/audit/rules.d/99-finalize.rules
       owner: root
       group: root
       mode: 0600
   - name: 4.1.17 Ensure the audit configuration is immutable
     template:
       src: files/templates/auditd/11-init.rules.j2
       dest: /etc/audit/rules.d/11-init.rules
       owner: root
       group: root
       mode: 0600
     notify:
       - audit rules load
       - auditd restart
 ignore_errors: yes
 tags:
   - section4
   - level_2_server
   - level_2_workstation
   - 4.1.17
# 4.2 Configure Logging
# 4.2.1 Configure rsyslog
# 4.2.1.1 Ensure rsyslog is installed
- name: 4.2.1.1 Ensure rsyslog is installed
 apt:
   name: rsyslog
   state: present
   install_recommends: false
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - 4.2.1.1
# 4.2.1.2 Ensure rsyslog Service is enabled
- name: 4.2.1.2 Ensure rsyslog Service is enabled
 service:
   name: rsyslog
   enabled: yes
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - 4.2.1.2
# 4.2.1.3 Ensure logging is configured
- name: 4.2.1.3 Ensure logging is configured
 blockinfile:
   path: /etc/rsyslog.conf
   backup: yes
   block: |
     *.emerg                 :omusrmsg:*
     mail.*                  -/var/log/mail
     mail.info               -/var/log/mail.info
     mail.warning            -/var/log/mail.warn
     mail.err                 /var/log/mail.err
     news.crit               -/var/log/news/news.crit
     news.err                -/var/log/news/news.err
```

```
     news.notice             -/var/log/news/news.notice
     *.=warning;*.=err       -/var/log/warn
     *.crit                   /var/log/warn
     *.*;mail.none;news.none -/var/log/messages
     local0,local1.*         -/var/log/localmessages
     local2,local3.*         -/var/log/localmessages
     local4,local5.*         -/var/log/localmessages
     local6,local7.*         -/var/log/localmessages
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - 4.2.1.3
# 4.2.1.4 Ensure rsyslog default file permissions configured
# It is important to ensure that log files have the correct permissions to ensure that sensitive data
is archived and protected.
- name: 4.2.1.4 Ensure rsyslog default file permissions configured
 lineinfile:
   dest: /etc/rsyslog.conf
   regexp: '^\$FileCreateMode'
   line: "$FileCreateMode 0640"
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - 4.2.1.4
# 4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host
# # Storing log data on a remote host protects log integrity from local attacks. If an attacker gains
root access on the local system, they could tamper with or remove log data that is stored on the local
system
- name: 4.2.1.5 Ensure rsyslog default file permissions configured
 lineinfile:
   path: /etc/rsyslog.conf
   backup: yes
   block: |
     *.* action(type="omfwd" target="{{ remoteSyslog.host }}" port="{{ remoteSyslog.port }}"
protocol="{{ remoteSyslog.protocol }}" action.resumeRetryCount="100" queue.type="LinkedList"
queue.size="1000")
 when: remoteSyslog.enable == True
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - 4.2.1.5
# 4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts.
# The guidance in the section ensures that remote log hosts are configured to only accept rsyslog data
from hosts within the specified domain and that those systems that are not designed to be log hosts do
not accept any remote rsyslog messages. This provides protection from spoofed log data and ensures that
system administrators are reviewing reasonably complete syslog data in a central location.
- name: 4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts.
 block:
   - name: 4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts. | $ModLoad
     lineinfile:
       dest: /etc/rsyslog.conf
       regexp: '^\$ModLoad'
       line: "$ModLoad imtcp"
   - name: 4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts. |
$InputTCPServerRun
     lineinfile:
       dest: /etc/rsyslog.conf
       regexp: '^\$InputTCPServerRun'
       line: "$InputTCPServerRun 514"
     notify:
       - rsyslog restart
 tags:
   - section4
   - level_1_server
   - level_1_workstation
```

```
   - 4.2.1.6
# 4.2.2 Configure journald
# 4.2.2.1 Ensure journald is configured to send logs to rsyslog
# Storing log data on a remote host protects log integrity from local attacks. If an attacker gains
root access on the local system, they could tamper with or remove log data that is stored on the local
system.
- name: 4.2.2.1 Ensure journald is configured to send logs to rsyslog
 lineinfile:
   dest: /etc/systemd/journald.conf
   regexp: "(#)?ForwardToSyslog=(yes|no)"
   line: ForwardToSyslog=yes
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - 4.2.2.1
# 4.2.2.2 Ensure journald is configured to compress large log files
- name: 4.2.2.2 Ensure journald is configured to compress large log files
 lineinfile:
   dest: /etc/systemd/journald.conf
   regexp: "(#)?Compress=(yes|no)"
   line: Compress=yes
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - 4.2.2.2
# 4.2.2.3 Ensure journald is configured to write logfiles to persistent disk
# Writing log data to disk will provide the ability to forensically reconstruct events which may have
impacted the operations or security of a system even after a system crash or reboot.
- name: 4.2.2.3 Ensure journald is configured to write logfiles to persistent disk
 lineinfile:
   dest: /etc/systemd/journald.conf
   regexp: "(#)?Storage=(auto|persistent)"
   line: Storage=persistent
 notify:
   - journald restart
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - 4.2.2.3
# 4.2.3 Ensure permissions on all logfiles are configured
# It is important to ensure that log files have the correct permissions to ensure that sensitive data
is archived and protected.
- name: 4.2.3 Ensure permissions on all logfiles are configured
 shell: |
   find /var/log -type f -exec chmod g-wx,o-rwx "{}" + -o -type d -exec chmod g-w,o-rwx "{}" +
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - 4.2.3
# 4.3 Ensure logrotate is configured
# # By keeping the log files smaller and more manageable, a system administrator can easily archive
these files to another system and spend less time looking through inordinately large log files.
- name: 4.3 Ensure logrotate is configured
 replace:
   path: /etc/logrotate.d/rsyslog
   regexp: '^(\s*)(daily|weekly|monthly|yearly)$'
   replace: "\\1{{ logrotate_policy }}"
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - _4.3
# 4.4 Ensure logrotate assigns appropriate permissions
```

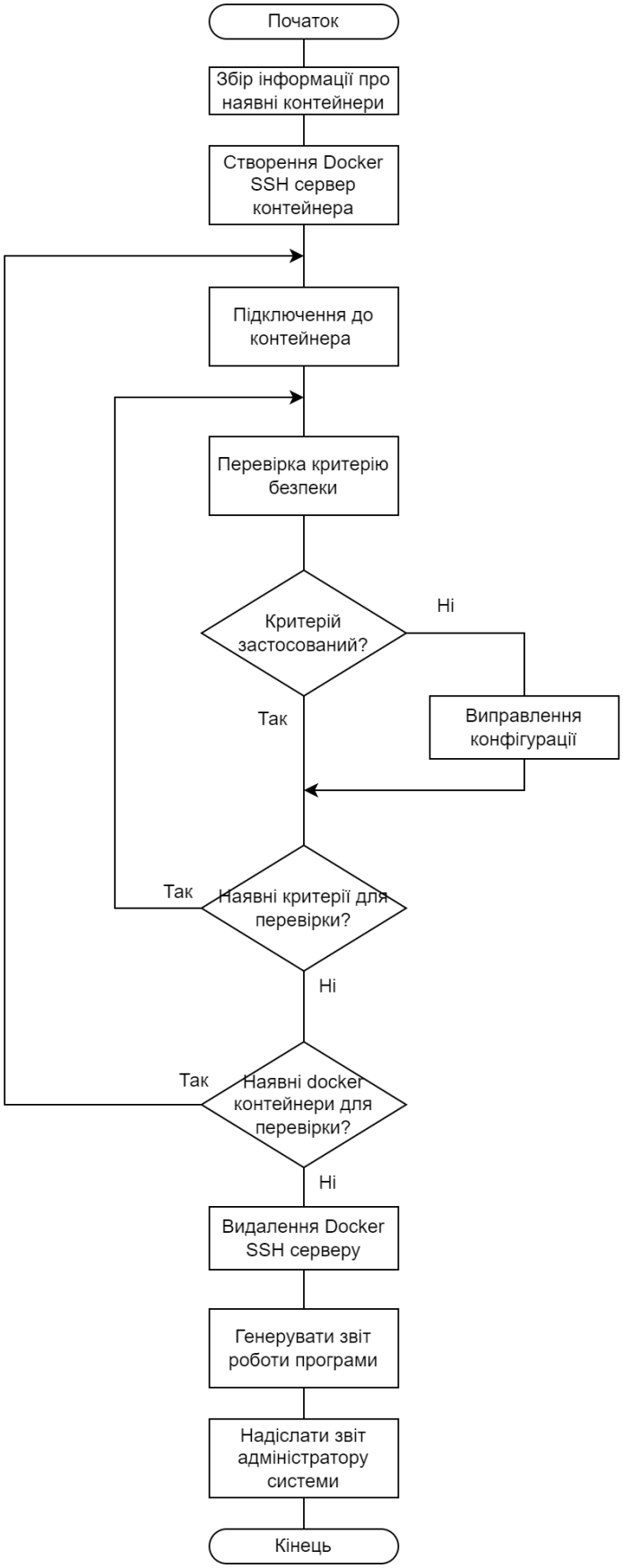
```
# It is important to ensure that log files have the correct permissions to ensure that sensitive data
is archived and protected.
- name: 4.4 Ensure logrotate assigns appropriate permissions
 lineinfile:
   dest: /etc/logrotate.conf
   regexp: "^create"
   line: "create 0640 root utmp"
 notify:
   - journald restart
 tags:
   - section4
   - level_1_server
   - level_1_workstation
   - _4.4
```

Додаток Д

ІЛЮСТРАТИВНА ЧАСТИНА

МЕТОД ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ DOCKER-КОНТЕЙНЕРІВ

Алгоритм роботи програми



Рівні середовища Docker

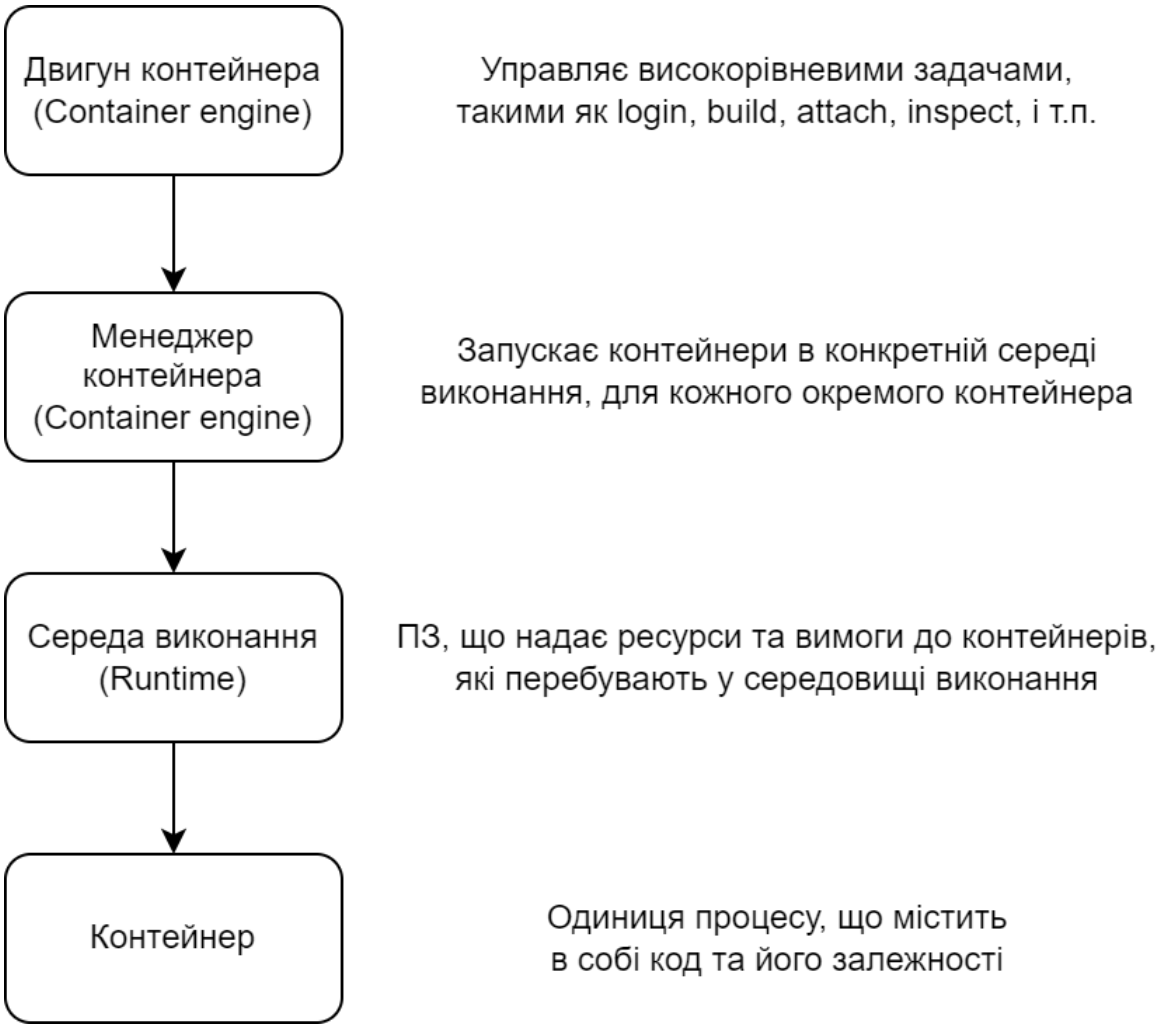
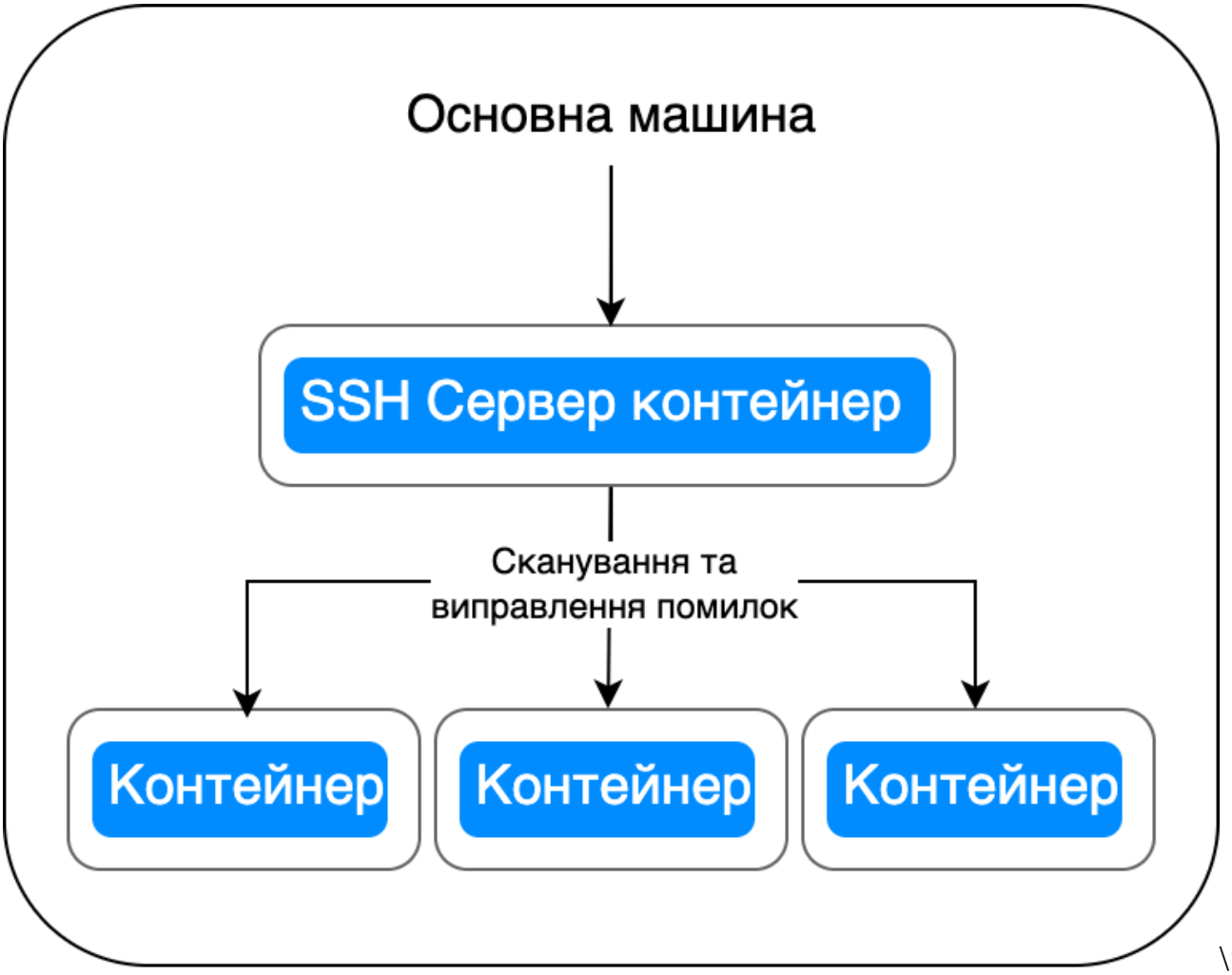
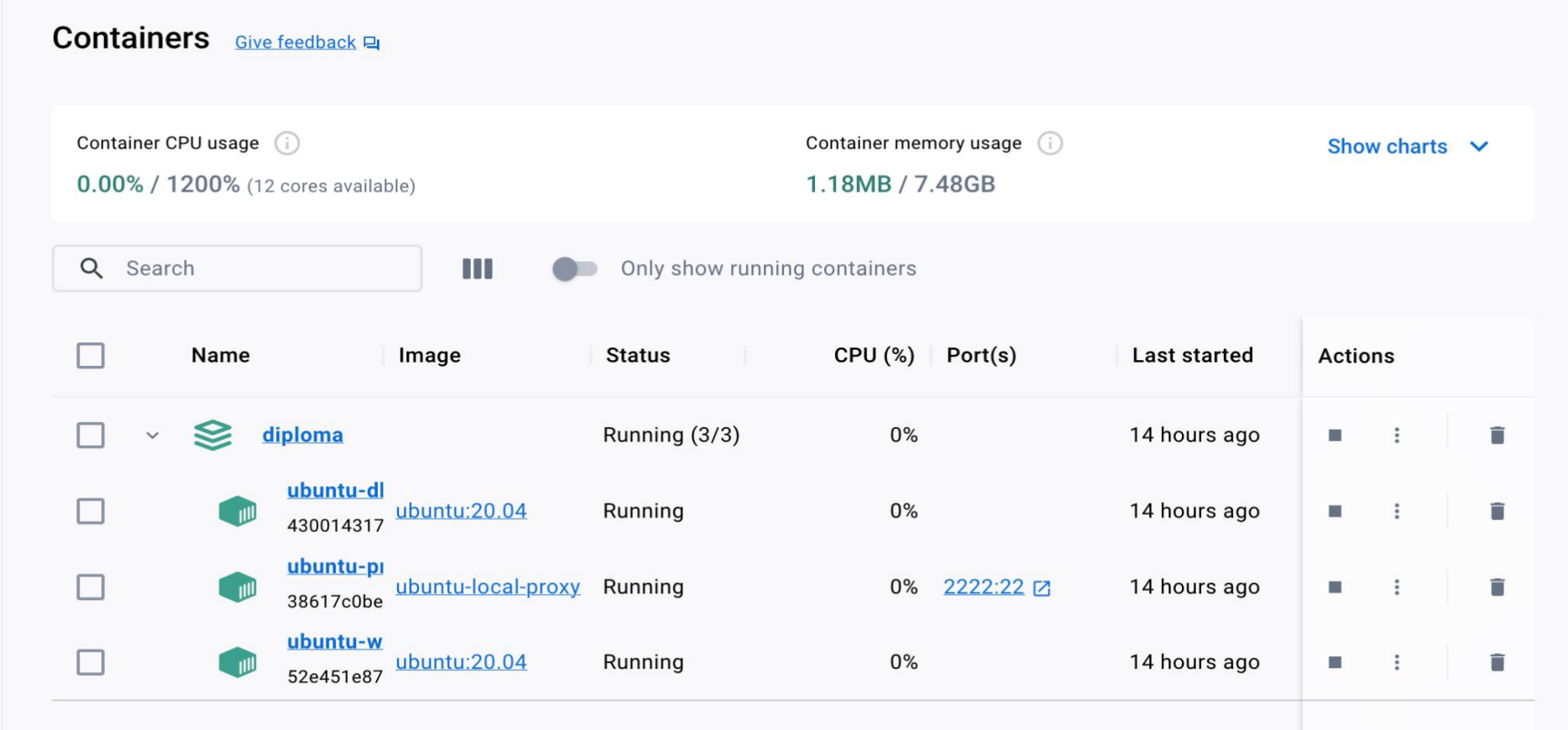


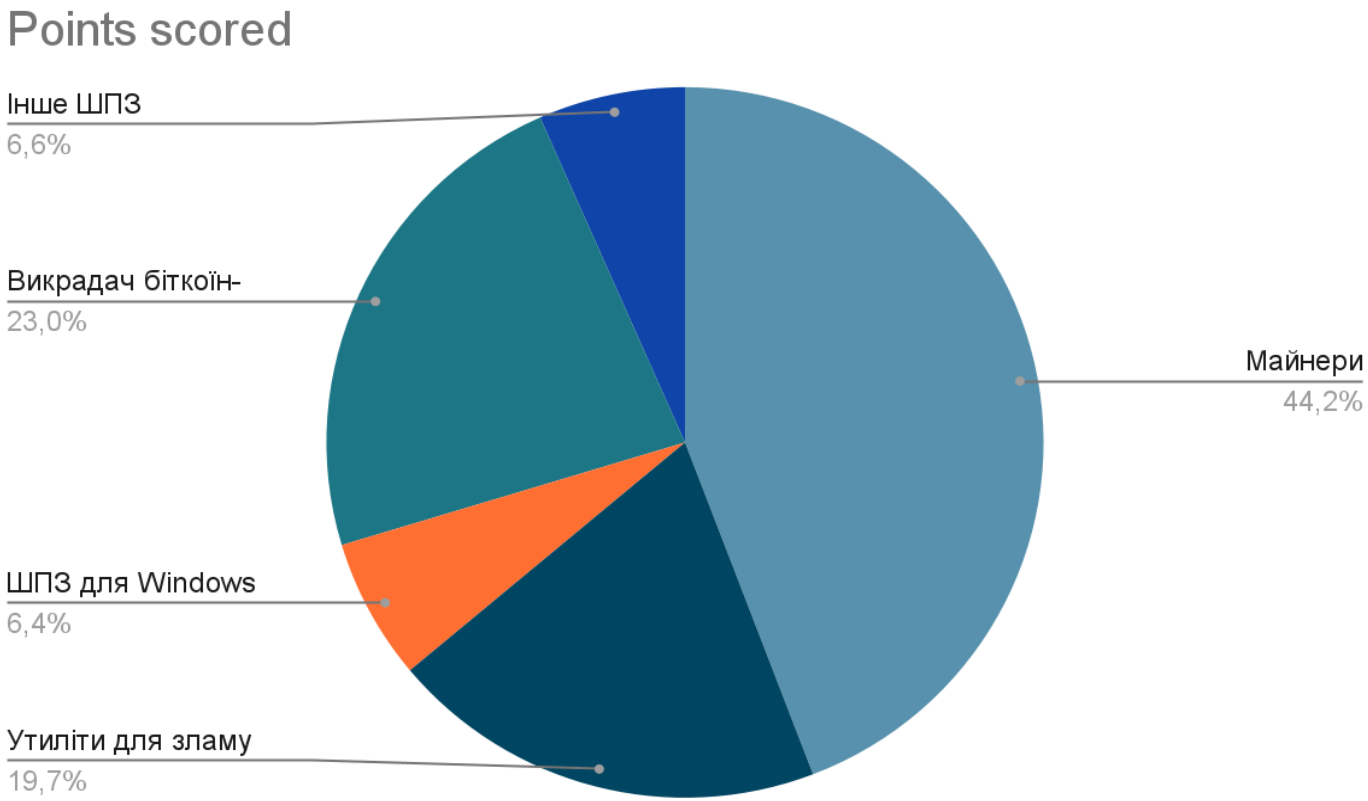
Схема взаємодії використовуваних компонентів



Запущені Docker-контейнери для тестування



Діаграма розподілення типів ШПЗ у образах Docker-контейнерів



Розрахунки приросту коефіцієнту захищеності контейнерів

Номер секції	Позначення коефіцієнта	Розрахунки	Коефіцієнт захищеності	Приріст захищеності
Секція 1	$K_{\text{до}}$	$\frac{65}{65+34+11+3}$	$\frac{65}{113}=0.57$	+0.3
	$K_{\text{після}}$	$\frac{65+34}{65+34+11+3}$	$\frac{99}{113}=0.87$	
Секція 2	$K_{\text{до}}$	$\frac{28}{28+4+10}$	$\frac{28}{42}=0.66$	+0.1
	$K_{\text{після}}$	$\frac{28+4}{28+4+10}$	$\frac{32}{42}=0.76$	
Секція 3	$K_{\text{до}}$	$\frac{38}{38+33+14}$	$\frac{38}{85}=0.44$	+0.39
	$K_{\text{після}}$	$\frac{38+33}{38+33+14}$	$\frac{71}{85}=0.83$	
Секція 4	$K_{\text{до}}$	$\frac{42}{42+37+1}$	$\frac{42}{80}=0.52$	+0.45
	$K_{\text{після}}$	$\frac{42+37}{42+37+1}$	$\frac{79}{80}=0.98$	
Секція 5	$K_{\text{до}}$	$\frac{70}{70+61+3}$	$\frac{70}{134}=0.52$	+0.45
	$K_{\text{після}}$	$\frac{70+61}{70+61+3}$	$\frac{131}{134}=0.97$	
Секція 6	$K_{\text{до}}$	$\frac{56}{56+49+6}$	$\frac{56}{111}=0.50$	+0.44
	$K_{\text{після}}$	$\frac{56+49}{56+49+6}$	$\frac{105}{111}=0.94$	

Результат сканування образа Ubuntu утилітою Trivy

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2		coreutils: Non-privileged session can escape to the parent session in chroot https://avd.aquasec.com/nvd/cve-2016-2781
gpgv	CVE-2022-3219			2.2.19-3ubuntu2.2		denial of service issue (resource consumption) using compressed packets https://avd.aquasec.com/nvd/cve-2022-3219
libc-bin	CVE-2016-20013			2.31-0ubuntu9.12		sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of... https://avd.aquasec.com/nvd/cve-2016-20013
	CVE-2023-4806		fixed		2.31-0ubuntu9.14	glibc: potential use-after-free in getaddrinfo() https://avd.aquasec.com/nvd/cve-2023-4806
	CVE-2023-4813					glibc: potential use-after-free in gaih_inet() https://avd.aquasec.com/nvd/cve-2023-4813
libc6	CVE-2016-20013		affected			sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of... https://avd.aquasec.com/nvd/cve-2016-20013
	CVE-2023-4806		fixed		2.31-0ubuntu9.14	glibc: potential use-after-free in getaddrinfo() https://avd.aquasec.com/nvd/cve-2023-4806
	CVE-2023-4813					glibc: potential use-after-free in gaih_inet() https://avd.aquasec.com/nvd/cve-2023-4813
liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1		Denial of service via decompression of crafted file https://avd.aquasec.com/nvd/cve-2020-22916
libpcre3	CVE-2017-11164	LOW		2:8.39-12ubuntu0.1		OP_KETRMAX feature in the match function in pcre_exec.c https://avd.aquasec.com/nvd/cve-2017-11164
libsystemd0	CVE-2023-26604			245.4-4ubuntu3.22		systemd: privilege escalation via the less pager https://avd.aquasec.com/nvd/cve-2023-26604
libudev1						
login	CVE-2013-4235			1:4.8.1-1ubuntu5.20.04.4		shadow-utils: TOCTOU race conditions by copying and removing directory trees https://avd.aquasec.com/nvd/cve-2013-4235
	CVE-2023-29383					Improper input validation in shadow-utils package utility chfn https://avd.aquasec.com/nvd/cve-2023-29383
passwd	CVE-2013-4235					shadow-utils: TOCTOU race conditions by copying and removing directory trees https://avd.aquasec.com/nvd/cve-2013-4235
	CVE-2023-29383					Improper input validation in shadow-utils package utility chfn https://avd.aquasec.com/nvd/cve-2023-29383
tar	CVE-2023-39804	MEDIUM		1.30+dfsg-7ubuntu0.20.04.3		[A stack overflow vulnerability exists in GNU Tar up to including v1.34.... https://avd.aquasec.com/nvd/cve-2023-39804