МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ДЛЯ ОЦІНКИ БЕЗПЕКИ ХМАРНИХ ІНФРАСТРУКТУР ТА СЕРВІСІВ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олександр РОМАНОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Олександр РОМАНОВ
Ім’я, ПРІЗВИЩЕ

Керівник: Дмитро РАБЧУН
К.т.н. Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
Д.т.н., проф. Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Романову Олександру Андрійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи тестування на проникнення для оцінки безпеки хмарних інфраструктур”,
керівник кваліфікаційної роботи РАБЧУН Дмитро, к.т.н.
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від 27.02.24 № 36.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *міжнародні стандарти, наукова та технічна література, методи та засоби тестування хмарних інфраструктур та сервісів, методології тестування на проникнення, вразливості притаманні хмарним середовищам.*

4. Перелік питань, які мають бути розроблені:

4.1. Визначити поняття та особливості хмарної інфраструктури та сервісів, їх безпекову складову.

4.2. Дослідити основні методи тестування захищенності хмарних інфраструктур та сервісів.

4.3. Вивчити інструменти та методи тестування захищенності мобільних додатків, розробити практичні рекомендації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	26.03.2024	
3.	Дослідження загальних відомостей про поняття та безпеку хмарних інфраструктур та сервісів.	02.04.2024	
4.	Дослідження основних методів тестування захищенності хмарних інфраструктур та сервісів.	16.04.2024	
5.	Вивчення інструментів та методів покращення тестування на проникнення хмарних інфраструктур та сервісів.	12.05.2024	
6.	Розробка рекомендацій для тестування захищенності хмарних інфраструктур та сервісів.	20.05.2024	
7.	Формулювання висновків за результатами проведеного дослідження.	26.05.2024	
8.	Оформлення роботи.	30.05.2024	
9.	Оформлення презентації.	03.06.2024	
10.	Отримання рецензії на роботу.	03.06.2024	
11.	Захист в ДЕК.	10.06.2024	

Здобувач вищої освіти _____ Олександр РОМАНОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Романов О.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи тестування на проникнення для оцінки безпеки хмарних інфраструктур"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач РОМАНОВ Олександр у кваліфікаційній роботі дослідив загальні відомості про поняття та безпеку хмарних інфраструктур та сервісів, дослідив основні методи тестування захищення хмарних інфраструктур та сервісів, вивчив інструменти та методи тестування захищення хмар, розробив практичні рекомендації за темою дослідження.

РОМАНОВ Олександр показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на одній конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача РОМАНОВА Олександра на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Романов О.А. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти РОМАНОВА Олександра
на тему “Методи тестування на проникнення для оцінки безпеки хмарних інфраструктур та сервісів”

Актуальність. Стрімкий, розвиток хмарних технологій та збільшення кількості користувачів, які все частіше обирають хмарні рішення замість традиційних. Це зумовлює необхідність забезпечення високого рівня кібербезпеки, оскільки хмари часто містять конфіденційну інформацію та особисті дані. Тестування захищеності допомагає виявляти та усувати вразливості, знижуючи ризик кібератак та зловмисного використання даних.

Отже, дослідження методів тестування захищенності хмарних інфраструктур та сервісів є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено загальні відомості про поняття та безпеку хмарних інфраструктур та сервісів.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу: близько 40 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо ефективного тестування захищенності хмарних інфраструктур та сервісів.

Недоліки.

Доцільно було б приділити більше уваги практичному застосуванню розроблених рекомендацій для тестування захищенності хмарних інфраструктур та сервісів.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач РОМАНОВ Олександр заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Галина ГАЙДУР
к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена аналізу та вдосконаленню методів тестування захищенності мобільних додатків. Робота складається зі вступу, трьох розділів, що містять 14 рисунків, висновків і списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 76 аркушів, з яких 6 аркуші займають перелік умовних скорочень та список використаних джерел.

Метою роботи є розробка рекомендацій для підвищення ефективності методів тестування на проникнення для оцінки безпеки хмарних інфраструктур та сервісів.

Об'єктом дослідження є методи тестування захищенності хмарних інфраструктур та сервісів.

Предмет дослідження – механізми оцінки безпеки хмарних інфраструктур та сервісів шляхом тестування на проникнення.

Методи дослідження. Для вирішення поставленого вище наукового завдання в роботі були використані методи аналізу, порівняння, класифікації, системного підходу до вдосконалення методів тестування захищенності хмарних інфраструктур та сервісів.

Як результат у роботі проаналізовано особливості та поняття хмарних інфраструктур та сервісів, досліджено основні принципи тестування захищенності хмар, вивчено методи тестування захищенності та розроблено практичні рекомендації.

Галузь застосування. Розроблені рекомендації можуть бути використані при проведенні тестування хмарних інфраструктур.

Ключові слова: ТЕСТУВАННЯ НА ПРОНИКНЕННЯ, ХМАРНІ ІНФРАСТРУКТУРИ, ХМАРНІ СЕРВІСИ, БЕЗПЕКА ХМАР, ВРАЗЛИВОСТІ, ЕТИЧНИЙ ХАКІНГ, ТЕСТУВАННЯ ЗАХИЩЕННОСТІ.

ABSTRACT

The qualification work is devoted to the analysis and improvement of data encryption methods in cloud computing. The work consists of an introduction, three chapters containing 14 figures, conclusions and the list of references containing 45 items. The total volume of the work is 76 pages, of which 6 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to develop recommendations for improving the effectiveness of penetration testing methods for assessing the security of cloud infrastructures and services.

The object the study are methods of testing the security of cloud infrastructures and services.

The subject of the study are mechanisms for assessing the security of cloud infrastructures and services through penetration testing.

Research methods. To solve the above scientific task, the paper used methods of analysis, comparison, classification, and a systematic approach to improving the methods of assessing the security of cloud infrastructures and services.

As a result, the paper analyzes the features and concepts of cloud infrastructures and services, explores the basic principles of cloud security testing, studies security testing methods, and develops practical recommendations.

Field of application. The developed recommendations can be used when testing cloud infrastructures.

Keywords: PENETRATION TESTING, CLOUD INFRASTRUCTURES, CLOUD SERVICES, CLOUD SECURITY, VULNERABILITIES, ETHICAL HACKING, SECURITY TESTING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
SECaaS	Security as a Service
FaaS	Function as a Service
GCP	Google Cloud Platform

ВСТУП

Актуальність теми. Стрімкий, розвиток х технологій та збільшення кількості користувачів, які залежать від мобільних пристроїв у своєму повсякденному житті. Це зумовлює необхідність забезпечення високого рівня кібербезпеки, оскільки мобільні додатки часто містять конфіденційну інформацію та особисті дані. Тестування захищеності допомагає виявляти та усувати вразливості, знижуючи ризик кібератак та зловмисного використання даних.

Отже, дослідження методів тестування захищенності хмарних інфраструктур та сервісів є актуальним науковим завданням.

Метою роботи є розробка рекомендацій для підвищення ефективності методів тестування на проникнення для оцінки безпеки хмарних інфраструктур та сервісів.

Об’єктом дослідження є методи тестування захищенності хмарних інфраструктур та сервісів.

Предмет дослідження – механізми оцінки безпеки хмарних інфраструктур та сервісів шляхом тестування на проникнення.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати загальні відомості про поняття та безпеку хмарних інфраструктур та сервісів.
2. Дослідити основні методи тестування захищенності хмарних інфраструктур.
3. Проаналізувати інструменти та методи тестування захищенності хмарних інфраструктур та сервісів, розробити практичні рекомендації.

Методи дослідження. Для вирішення поставленого вище наукового завдання в роботі були використані методи аналізу, порівняння, класифікації, системного підходу до вдосконалення методів тестування захищенності хмарних

інфраструктур та сервісів.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити пошук вразливостей у хмарних інфраструктурах.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО ПОНЯТТЯ ТА БЕЗПЕКУ ХМАРНИХ ІНФРАСТРУКТУР ТА СЕРВІСІВ

1.1 Визначення понять хмарної інфраструктури та сервісів: їх види та призначення

Сучасний світ зазнає стрімких, невпинних змін, які також стосуються і сфери цифрових технологій. Серед них особливе місце посідають технології хмарних обчислень [1], які кардинально змінили підхід користувачів до розгортання інфраструктур та сервісів, як для потреб бізнесу, так і для власних. Користувачам відкриваються широкі можливості для розгортання потужних та захищених інфраструктур та сервісів без необхідності придбання та обслуговування власного "On-Premise" [2] обладнання. Це особливо зручно для великих підприємств, яким необхідно забезпечувати належну роботу значних інфраструктур, що є досить складною задачею, яка вимагає багато ресурсів. Таким чином, користувачі та організації мають змогу брати в аренду обладнання у третіх сторін, які й будуть займатися його підтримуванням, оновленням та захистом.

Втім, у той час як стрімко розвиваються технології, стрімко з'являються й вразливості у них, хмарні технології не є виключенням. Майже щодня знаходяться нові вразливості на базі яких зловмисниками розроблюються різноманітні вектори атак на інфраструктури та сервіси підприємств і користувачів. Для розробки ефективних методів захисту у хмарному середовищі необхідно перш за все розібратися з основними поняттями та видами хмарних інфраструктур та сервісів.

Хмарна інфраструктура — [3], [4] це складна та багатогранна система, яка включає в себе широкий спектр фізичних та віртуальних ресурсів, що забезпечують надійну та ефективну роботу хмарних сервісів. Вона є основою для створення гнучкого, масштабованого та доступного хмарного середовища, яке

може адаптуватися до змінних потреб бізнесу та користувачів. До основних елементів хмарної інфраструктури відносяться:

- **Сервери** — це не просто фізичні машини, але й потужні обчислювальні центри, які підтримують віртуальні машини та контейнери. Вони забезпечують необхідні обчислювальні потужності для запуску та підтримки широкого спектру додатків та сервісів, від простих веб-сайтів до складних аналітичних систем. Сервери можуть бути розміщені в спеціалізованих дата-центрах, які забезпечують оптимальні умови для їх роботи, включаючи охолодження, живлення та безпеку.
- **Мережева інфраструктура** є життєво важливою для забезпечення зв'язку між різними компонентами хмари, а також для підключення користувачів до хмарних сервісів. Вона включає в себе фізичні маршрутизатори, комутатори, а також програмно-налаштовані мережі (SDN), які дозволяють гнучко управляти мережевими потоками та оптимізувати роботу мережі відповідно до потреб користувачів та додатків.
- **Сховища даних** — це системи, які забезпечують швидкий доступ до даних, їх резервне копіювання та відновлення. Вони можуть використовувати різні типи носіїв, від традиційних жорстких дисків до швидкісних SSD, а також мережеві сховища (NAS/SAN), які дозволяють зберігати великі обсяги даних та забезпечувати їх доступність для користувачів з будь-якої точки світу.
- **Віртуалізація** є ключовою технологією у хмарній інфраструктурі, оскільки вона дозволяє створювати та управляти віртуальними машинами, які імітують роботу фізичних серверів. Це дозволяє оптимізувати використання обчислювальних ресурсів, ізолювати різні сервіси та додатки один від одного, а також швидко масштабувати ресурси відповідно до потреб користувачів.
- **Безпека в хмарній інфраструктурі** — це комплекс заходів, які забезпечують захист даних та ресурсів від різноманітних кіберзагроз. Вона

включає в себе як фізичні міжмережеві екрани, так і програмні системи виявлення вторгнень, управління доступом та шифрування даних, які допомагають запобігати несанкціонованому доступу та забезпечують конфіденційність інформації.

Необхідно зазначити, що хмарна інфраструктура може бути реалізована як у приватних, так і в публічних хмарах, або як гібридна модель, яка комбінує елементи обох [5], [6], [7]. Кожна з цих моделей має свої особливості, переваги та недоліки:

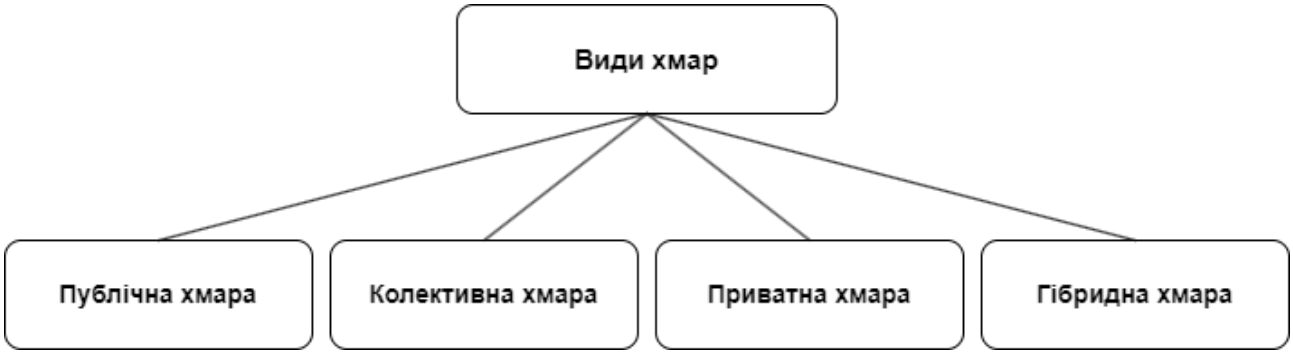

Рис. 1.1 Види реалізації хмарної інфраструктури

- **Публічна хмара (Public Cloud)** - це хмара, ресурси якої (сервери, сховища, додатки) надаються третім стороною-провайдером через інтернет і спільно використовуються багатьма клієнтами. До значних переваг можна віднести простоту в користуванні, низькі витрати на старт та оплату лише за використані ресурси. До недоліків можна віднести потенційні проблеми з продуктивністю через спільне використання ресурсів з іншими клієнтами, а також менший контроль над безпекою і конфігурацією розгорнутої інфраструктури. Прикладами публічних хмар є: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).
- **Колективна хмара (Community Cloud)** - це хмара, що використовується спільною групою користувачів, що мають подібні потреби та інтереси. Ця хмара створюється для підтримки специфічних вимог певної спільноти,

такої як організації в одному секторі, урядові установи, навчальні заклади або інші групи, що співпрацюють. Вона може бути керована безпосередньо користувачами або через обраних ними представників. Колективні хмари можуть бути розташовані локально (on-premises) або керуватися третьою стороною, що забезпечує відповідні ресурси та послуги. Плюсами використання є покращена співпраця між учасниками хмари, спільне використання ресурсів для економії коштів, а також гнучкість налаштувань хмарного середовища. До мінусів можна віднести складність налаштування, підвищені ризики безпеки через особливості середовища, а також можливі конфлікти інтересів між учасниками. Прикладами є Google Apps for Education, AWS GovCloud, DICOM Grid.

- **Приватна хмара (Private Cloud)** - це хмара, ресурси якої використовуються виключно однією організацією, а інфраструктура може розташовуватися як на території компанії, так і у зовнішнього провайдера. З переваг - повний контроль над безпекою та конфігурацією та можливість відповідати строгим вимогам до відповідності стандартам. З мінусів - вищі витрати на встановлення та обслуговування, а також складніше масштабування та управління. Прикладами приватних хмар є: VMware vSphere, OpenStack, Microsoft Azure Stack.
- **Гібридна хмара (Hybrid Cloud)** - це комбінація публічної та приватної хмар з інтегрованими можливостями управління даними та програмами між ними. Перевагами є гнучкість у розподілі навантажень між публічною та приватною хмарами, можливість використання переваг обох моделей, а також оптимізація витрат та ресурсів. Недоліками ж є складність в налаштуванні та управлінні, а також потреба в надійних засобах інтеграції та безпеки.

Реалізація хмарної інфраструктури може виконуватись різними способами, кожен з яких забезпечує організаціям гнучкість у виборі підходу, який

найкраще відповідає їхнім потребам та бізнес-цілям. Способами реалізації хмарної інфраструктури є:

- **Віртуалізація** - процесс створення віртуальних машин (VM) на фізичних серверах для оптимізації використання апаратних ресурсів. Сюди відносяться: VMware, KVM, Hyper-V.
- **Контейнери та оркестрація** - використання контейнерів для ізоляції додатків і середовищ виконання з метою забезпечення портативності та ефективності. Напр. Docker та Kubernetes.
- **Безсерверні обчислення (Serverless Computing)** - запуск коду у відповідь на події без управління серверами, з оплатою лише за фактичне використання. Прикладами є AWS Lambda, Azure Functions, Google Cloud Functions.
- **Платформи хмарного управління (Cloud Management Platforms)** - інструменти для управління хмарною інфраструктурою, включаючи моніторинг, автоматизацію та оркестрацію. Технологіями є VMware vRealize, OpenStack Horizon, Microsoft System Center.

Хмарні сервіси — це послуги, які надаються через інтернет з використанням хмарної інфраструктури [8].

Вони дозволяють користувачам отримувати доступ до програмного забезпечення, обчислювальних ресурсів, сховищ даних та інших IT-ресурсів без потреби в установці та управлінні фізичним обладнанням. Вони також сприяють інноваціям, оскільки розробники та IT-спеціалісти мають можливість швидко розгортати та тестувати нові програми та сервіси. Це стимулює експериментування та прискорює впровадження нових технологій, що може призвести до революційних змін у багатьох галузях. Крім того, хмарні сервіси забезпечують високий рівень безпеки та надійності, оскільки провайдери хмарних послуг інвестують значні ресурси в захист даних та інфраструктуру від

кібератак та фізичних пошкоджень [9], [10], [11], [12]. До основних типів хмарних сервісів входять:

Рис. 1.2 Види хмарних сервісів

- **Інфраструктура як послуга (IaaS)** - це модель хмарних послуг, яка дозволяє користувачам використовувати віртуалізовані обчислювальні ресурси через Інтернет. Ця модель пропонує значну гнучкість та масштабованість, оскільки користувачі можуть швидко збільшувати або зменшувати ресурси відповідно до своїх потреб. IaaS надає віртуальні машини, які імітують фізичні комп'ютери з власними операційними системами, дозволяючи користувачам запускати будь-які програми. Також користувачі мають доступ до сховищ даних, які можуть бути масштабовані для зберігання великих обсягів даних, та мережевих ресурсів, які забезпечують з'єднання між різними віртуалізованими сервісами. Серед найвідоміших провайдерів IaaS можна виділити Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP). Використання IaaS дозволяє компаніям оптимізувати витрати на IT-інфраструктуру, платячи лише за ті ресурси, які вони використовують, та уникати витрат на придбання та обслуговування фізичного обладнання. Це також сприяє швидкому розгортанню нових додатків та сервісів, забезпечуючи більшу ефективність та гнучкість бізнесу.
- **Платформа як послуга (Platform as a Service, PaaS)** - це категорія хмарних послуг, яка забезпечує розробникам комплексне середовище для створення, тестування та управління додатками без необхідності займатися складною

інфраструктурою, яка зазвичай пов'язана з процесом розробки. PaaS включає в себе не тільки обчислювальні ресурси, але й високорівневі інструменти, такі як системи управління базами даних, інструменти для управління версіями коду, інтеграційні сервіси та інші компоненти, які спрощують процес розробки. Користувачі PaaS можуть зосередитися на написанні коду та інноваціях, не турбуючись про підтримку операційної системи, мережевого обладнання, або безпеки серверів, оскільки всі ці аспекти управляються провайдером послуг. Приклади платформ PaaS включають Google App Engine, який дозволяє розробникам створювати додатки на інфраструктурі Google, Microsoft Azure App Services, що надає широкий спектр обчислювальних послуг та інтеграцій з іншими продуктами Microsoft, та Heroku, який підтримує кілька мов програмування та інтегрується з різними базами даних та сервісами. Використання PaaS може значно прискорити розробку та запуск додатків, а також знизити загальні витрати на інфраструктуру.

- **Програмне забезпечення як послуга (Software as a Service, SaaS)** - надає користувачам можливість доступу до програм через інтернет, що відкриває широкі можливості для масштабування та глобальної інтеграції. Завдяки централізованому хостингу, користувачі можуть уникнути багатьох технічних складнощів, пов'язаних з установкою та налаштуванням програм на індивідуальних комп'ютерах, що значно спрощує процес впровадження нових інструментів та сервісів. Тобто, користувачам не потрібно встановлювати та обслуговувати програми на своїх пристроях; вони просто використовують їх через веб-браузер. Найпоширенішими прикладами є Google Workspace (Gmail, Google Docs), Microsoft Office 365, Salesforce.
- **Безпека як послуга (Security as a Service)** - це модель надання послуг кібербезпеки через хмарні сервіси. Вона дозволяє організаціям отримувати послуги безпеки від сторонніх постачальників на основі передплати. Замість того, щоб інвестувати в інфраструктуру та персонал для забезпечення безпеки, компанії можуть використовувати хмарні сервіси для захисту своїх

даних і систем. SECaaS включає різноманітні послуги, такі як управління ідентифікацією та доступом (IAM), захист веб-додатків, захист електронної пошти, безпека мережі, управління вразливостями, моніторинг безпеки та багато іншого. Прикладами є Cloudflare, Splunk Cloud, CrowdStrike Falcon та ін.

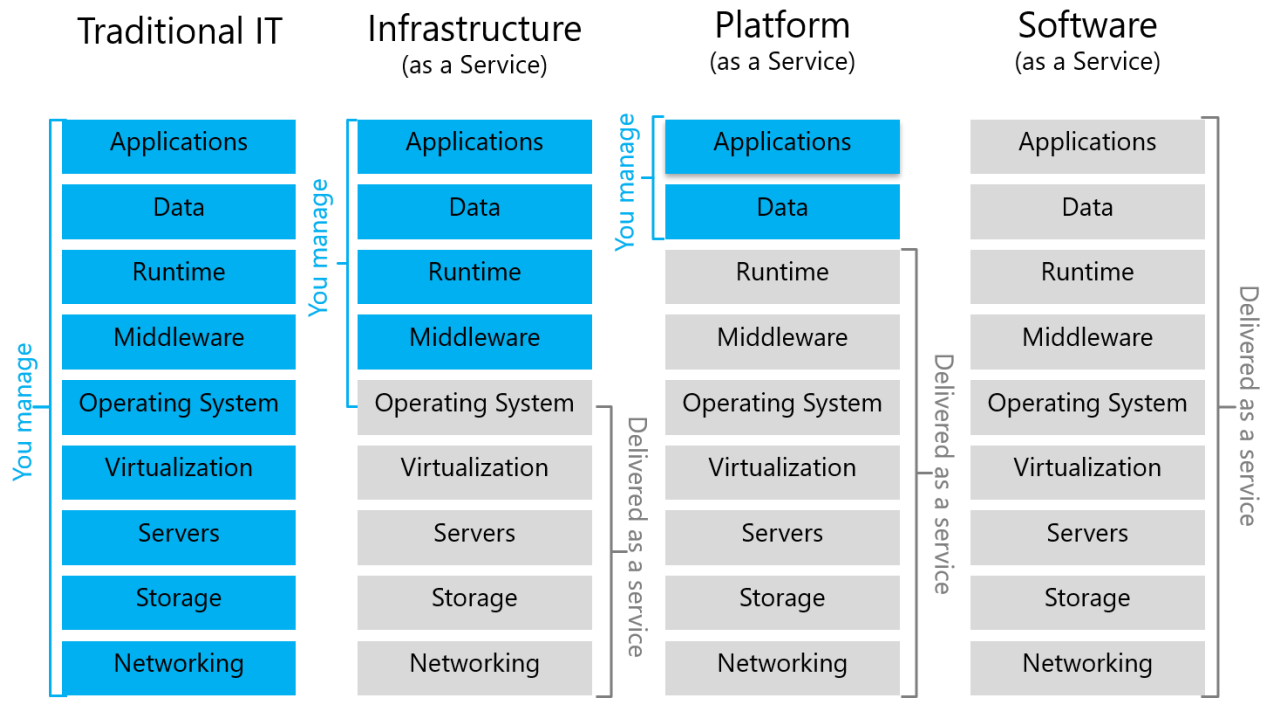

Рис. 1.3 Порівняння різних видів хмарних сервісів з традиційними сервісами [13].

Хмарні технології, які є важливою частиною сучасної IT-інфраструктури, пропонують гнучкість та масштабованість, але також стикаються з рядом викликів. Одним з основних є питання конфіденційності та безпеки даних. Це стосується здатності хмарних провайдерів захищати дані клієнтів від несанкціонованого доступу та забезпечувати їх цілісність. Залежність від інтернет-з'єднання також є критичною, оскільки перебої в мережі можуть призвести до втрати доступу до важливих даних та сервісів. Інтеграція з існуючими IT-системами може бути складною через різноманітність платформ та стандартів. Однак, з постійним розвитком технологій, таких як шифрування даних та розширені мережеві протоколи, багато з цих викликів можуть бути подолані. Підвищення рівня освіти та кваліфікації в галузі IT дозволяє фахівцям

краще розуміти та управляти хмарними ресурсами, забезпечуючи більш ефективну та безпечну роботу. Ринок хмарних технологій продовжує демонструвати зростання, що підтверджує їх збільшену популярність та ефективність. Це зростання також сприяє інноваціям та інвестиціям у секторі, що веде до постійного вдосконалення хмарних сервісів та інфраструктури. В результаті, хмарні технології стають все більш привабливими для різних видів бізнесу, від стартапів до великих корпорацій, які прагнуть до оптимізації своїх IT-операцій.

1.2 Поширені вразливості у хмарних інфраструктурах та сервісах

Безпека хмарних інфраструктур та сервісів є надзвичайно важливою у сучасному цифровому світі, де дані є новою валютою. Забезпечення безпеки даних, які зберігаються, передаються та обробляються в хмарі, вимагає комплексного підходу, що охоплює різноманітні аспекти та технології. Від правильної конфігурації безпеки, яка запобігає несанкціонованому доступу та витоку даних, до використання сучасних методів криптографії для захисту інформації під час її передачі та зберігання. Хмарні інфраструктури та сервіси, попри численні переваги, мають свої вразливості, які можуть стати серйозною загрозою для безпеки даних і систем.

Одним з найвідоміших проєктів, який описує найважливі загрози безпеки для хмарних середовищ, є OWASP Cloud Top 10 організації OWASP [14]. OWASP (Open Web Application Security Project) - це організація, яка зосереджується на покращенні безпеки програмного забезпечення. Вони створюють різні керівництва, інструменти та стандарти, які допомогають розробникам та організаціям захищати свої веб-додатки.

До переліку останньої версії OWASP Cloud Top 10, яка була розроблена у 2022 році, входять наступні ризики та вразливості:

CNAS01:2022 - Незахищені хмарні, контейнерні або оркестрові конфігурації
CNAS02:2022 - Недоліки ін'єкцій (рівень додатків, хмарні події, хмарні сервіси)
CNAS03:2022 - Неналежна автентифікація та авторизація
CNAS04:2022 - Недоліки конвеєра CI/CD та ланцюжка постачання програмного забезпечення
CNAS05:2022 - Незахищене зберігання секретів
CNAS06:2022 - Надмірно дозволені або незахищені мережеві політики
CNAS07:2022 - Використання компонентів з відомими уразливостями
CNAS08:2022 - Неналежне управління активами
CNAS09:2022 - Неадекватні ліміти квот на обчислювальні ресурси
CNAS10:2022 - Неефективне ведення журналів та моніторинг

Рис. 1.4 OWASP Top 10 Cloud - список поширених хмарних вразливостей

- **CNAS-1: Незахищені хмарні, контейнерні або оркестрові конфігурації**. CNAS-1 відноситься до набору проблем безпеки, які можуть виникнути в хмарних, контейнерних або оркестрових конфігураціях. Це включає загальнодоступні відра хмарного сховища, які можуть бути легко доступні для несанкціонованого доступу через неправильно налаштовані дозволи, створюючи значні ризики витоку даних. Неправильні дозволи на хмарних сховищах можуть дозволити неавторизованим користувачам завантажувати, змінювати або видаляти дані, що може призвести до порушення безпеки даних. Контейнери, які працюють від імені користувача root, можуть надати потенційним атакуючим повний контроль над контейнером, що може призвести до серйозних проблем безпеки. Крім того, якщо контейнер розділяє ресурси з хостом, такі як мережевий інтерфейс, це може створити додаткові вразливості. Незахищена конфігурація інфраструктури як коду (IaC) може призвести до автоматичного розгортання небезпечних конфігурацій, що може спричинити непередбачені безпекові проблеми.
- **CNAS-2: Недоліки ін'єкцій (рівень додатків, хмарні події, хмарні сервіси)**. CNAS-2 відноситься до недоліків ін'єкцій, які можуть виникати

на рівні додатків, під час хмарних подій, а також у хмарних сервісах. Ці недоліки можуть призвести до серйозних проблем з безпекою, оскільки вони дозволяють зловмисникам вводити шкідливий код, який може бути виконаний системою. SQL-ін'єкція є одним з найбільш відомих типів ін'єкцій, який дозволяє атакуючому маніпулювати запитами до бази даних, що може призвести до несанкціонованого доступу до даних або їх знищення. XXE, або XML External Entity, є типом атаки, що використовує обробку XML-файлів для виконання небажаних дій, таких як доступ до файлів, відправка запитів до зовнішніх систем, та інше. NoSQL ін'єкція схожа на SQL-ін'єкцію, але вона спрямована на бази даних NoSQL, які стають все більш популярними у сучасних додатках. Ін'єкція команд ОС дозволяє атакуючому виконувати довільні команди на сервері, що може призвести до повного контролю над системою. Безсерверна ін'єкція даних подій відноситься до атак, які використовують функції безсерверних архітектур, такі як AWS Lambda, для виконання шкідливого коду через події, що обробляються цими функціями.

- **CNAS-3: Неналежна автентифікація та авторизація**. CNAS-3 відноситься до проблем, пов'язаних з неналежною автентифікацією та авторизацією в системах кібербезпеки. Неавторизований доступ до API на мікросервісі може призвести до витоку конфіденційної інформації та зловмисного використання даних. Хмарні IAM (Identity and Access Management) повинні мати чітко визначені ролі та обмеження, щоб запобігти надмірно широким повноваженням, які можуть дозволити несанкціонований доступ до важливих ресурсів. Відсутність правил довіри до вузла-оркестратора, такого як Kubernetes, може дозволити несанкціоноване приєднання хостів до кластера, що створює ризики безпеки для всієї інфраструктури. Також критично важливо контролювати доступ до консолі оркестратора, оскільки неавторизований доступ може дозволити зловмисникам управляти розгортаннями та конфігураціями. Загалом, несанкціонований або надмірно дозволений доступ до

оркестратора може призвести до серйозних порушень безпеки, включаючи втрату даних, порушення цілісності системи та зловмисні атаки.

- **CNAS-4: Недоліки конвеєра CI/CD та ланцюжка постачання програмного забезпечення**. Конвеєри CI/CD є критично важливими для сучасних процесів розробки програмного забезпечення, оскільки вони автоматизують збирання, тестування та розгортання коду. Однак, існують певні недоліки, які можуть підвищити ризики безпеки та ефективності. Недостатня автентифікація в системах CI/CD може дозволити несанкціонований доступ до конвеєрів, що може призвести до змін у коді або витоку конфіденційної інформації. Використання ненадійних або застарілих образів може включати вразливості, які зловмисники можуть експлуатувати. Незахищені канали зв'язку з реєстрами можуть бути перехоплені, що дозволяє атакуючим модифікувати образи або вводити шкідливий код. Надмірно широкий доступ до реєстру може призвести до того, що занадто багато користувачів матимуть можливість змінювати або завантажувати образи, що збільшує ризик компрометації. Використання єдиного середовища для виконання завдань CI/CD для проектів з різними рівнями безпеки може призвести до того, що недоліки одного проекту можуть вплинути на інші проекти.
- **CNAS-5: Незахищене зберігання секретів**. CNAS-5 відноситься до проблем безпеки, пов'язаних з незахищеним зберіганням секретів, які можуть включати паролі, ключі API, токени доступу та інші чутливі дані. Зберігання секретів оркестратора в незашифрованому вигляді створює значні ризики, оскільки це може дозволити несанкціонований доступ до важливих системних компонентів. Ключі або паролі API, що зберігаються в контейнерах без належного шифрування, також піддаються ризику витоку, що може призвести до компрометації веб-сервісів та інших онлайн-ресурсів. Жорстко закодовані секрети в коді додатків є поганою практикою, оскільки вони можуть бути легко виявлені під час аудиту коду або в разі витоку кодової бази. Використання застарілих методів

шифрування або кодування замість шифрування може не забезпечити достатнього рівня захисту, оскільки сучасні методи криптоаналізу можуть легко їх зламати.

- **CNAS-6: Надмірно дозволені або незахищені мережеві політики**. CNAS-6 відноситься до проблематики надмірно дозволених або незахищених мережевих політик, які можуть становити значний ризик для безпеки інформаційних систем. Надмірно вільний зв'язок між Cloud Pod'ами може призвести до неконтрольованого розповсюдження шкідливого коду або несанкціонованого доступу до даних. Відкритість внутрішніх мікросервісів для публічного Інтернету створює потенційні точки входу для зловмисників. Відсутність чітко визначеної сегментації мережі ускладнює контроль та управління доступом, а також збільшує складність виявлення та реагування на інциденти безпеки. Нешифровані наскрізні комунікації можуть бути перехоплені, що ставить під загрозу конфіденційність передаваних даних. Неконтрольований мережевий трафік до невідомих або потенційно зловмисних доменів відкриває шлях для фішингових атак, розповсюдження шкідливого ПЗ та інших кіберзагроз.
- **CNAS-7: Використання компонентів з відомими уразливостями**. CNAS-7 описує проблему використання компонентів з відомими уразливостями, яка є однією з найбільш критичних ризиків безпеки веб-додатків. Це стосується вразливих сторонніх пакетів з відкритим вихідним кодом, де зловмисники можуть використовувати відомі уразливості для проведення атак. Вразливі версії компонентів додатків також можуть бути експлуатовані, що підкреслює необхідність регулярного оновлення та патчування програмного забезпечення. Крім того, використання відомих вразливих образів контейнерів може призвести до серйозних проблем безпеки, оскільки контейнери часто використовуються для розгортання додатків у хмарному середовищі.

- **CNAS-8: Неналежне управління активами**. CNAS-8, яке стосується неналежного управління активами, є критично важливим аспектом у сфері кібербезпеки. Недокументовані мікросервіси та API можуть створювати значні ризики, оскільки вони ускладнюють процеси ідентифікації, управління та захисту від потенційних загроз. Без належної документації, команди безпеки не можуть ефективно відстежувати та контролювати всі активи, що призводить до слабких місць у захисті інформації. Застарілі та некеровані хмарні ресурси також є проблемою, оскільки вони можуть містити вразливості, які не були виправлені через відсутність оновлень безпеки. Це створює можливості для кібератак та витоку даних. Управління активами вимагає ретельного підходу до інвентаризації, класифікації та моніторингу всіх активів, щоб забезпечити їх безпеку та відповідність нормативним вимогам.
- **CNAS-9: Неадекватні ліміти квот на «обчислювальні» ресурси**. CNAS-9 відноситься до проблеми неадекватних лімітів квот на обчислювальні ресурси в середовищі хмарних обчислень. Це може призвести до ситуацій, коли контейнери працюють без чітко визначених обмежень на використання ресурсів, що, у свою чергу, може спричинити перевантаження системи або навіть її збій. Наприклад, якщо контейнери не мають прив'язки до ресурсів, вони можуть споживати більше обчислювальної потужності, ніж це необхідно, що може негативно вплинути на інші процеси в системі. Також, встановлення надмірної квоти запитів на API може призвести до зловживань, коли один користувач або процес може використовувати більшу частину доступних ресурсів, залишаючи інших користувачів з обмеженими можливостями для виконання їхніх задач. Це створює ризики для безпеки та ефективності хмарних сервісів, оскільки надмірне використання ресурсів одним елементом може вплинути на загальну працездатність системи.
- **CNAS-10: Неефективне ведення журналів та моніторинг (наприклад, активність під час виконання)**. CNAS-10 вказує на проблеми з

моніторингом та веденням журналів у системах, що може призвести до втрати контролю над важливими процесами та потенційно створити ризики для безпеки. Неефективне ведення журналів може ускладнити виявлення та виправлення помилок, а також затруднити відстеження дій користувачів та системних процесів. Відсутність моніторингу активності контейнера або хост-процесу може призвести до непомічених збоїв або несанкціонованої діяльності. Недостатній контроль за мережевими комунікаціями між мікросервісами може відкрити шлях для мережевих атак та порушень даних. Ігнорування моніторингу споживання ресурсів може призвести до перевантаження системи, що в свою чергу може вплинути на доступність критичних ресурсів. Нарешті, відсутність контролю за розповсюдженням конфігурації оркестрування та застарілих конфігурацій може спричинити за собою використання неправильних налаштувань, що може вплинути на стабільність та безпеку всієї системи.

Вищенаведений перелік ризиків та вразливостей комплексно описує усі ті аспекти хмарних середовищ, на які варто звертати увагу розробникам та організаціям. Розуміння та усунення цих ризиків та вразливостей є критично важливим для забезпечення безпеки хмарних інфраструктур та сервісів. Компанії повинні впроваджувати належні заходи захисту, регулярно проводити аудит безпеки та забезпечувати відповідність регуляторним вимогам, щоб зменшити ризики та захистити свої дані від можливих загроз [15].

1.3 Сучасні вимоги до безпеки хмарних інфраструктур та сервісів

Сучасні вимоги до безпеки хмарних інфраструктур та сервісів охоплюють комплексні заходи, які забезпечують захист даних на різних рівнях: від загальних стандартів, таких як ISO/IEC 27001:2022 [16], до специфічних національних законодавств. Новий стандарт ISO/IEC 27001:2022, наприклад, включає оновлені контролі для хмарних сервісів, які допомагають організаціям систематично

визначати процеси придбання, використання, управління та виходу з хмарних сервісів.

Загальні вимоги створюють основу для забезпечення базового рівня безпеки, який є обов'язковим для всіх користувачів та організацій. Вони включають ідентифікацію та управління доступом, конфігурацію системи, а також заходи проти ненавмисного розкриття даних. Специфічні вимоги, які можуть бути закріплені у вигляді національних законів та постанов, зазвичай стосуються певних секторів або типів даних, як, наприклад, персональні дані [17] або фінансова інформація.

В умовах, які швидко змінюються, таких як воєнний стан, можуть бути введені тимчасові постанови, що регулюють використання хмарних сервісів специфічними групами, такими як банківські установи [18]. Ці заходи дозволяють адаптуватися до викликів, які виникають внаслідок надзвичайних ситуацій, забезпечуючи при цьому безперервність бізнесу та захист критично важливої інформації.

Важливо, що організації повинні не лише впроваджувати ці вимоги, але й регулярно переглядати та оновлювати свої політики безпеки, щоб відповідати новим технологічним реаліям та загрозам. Це включає моніторинг нових ризиків, оцінку ефективності існуючих заходів безпеки та впровадження вдосконалених контрольних механізмів. Такий підхід дозволяє забезпечити високий рівень захисту даних у хмарних сервісах, які стають все більш інтегрованими в повсякденні бізнес-процеси.

Загальними ж вимогами [19] до забезпечення безпеки хмарних інфраструктур та сервісів є наступні:

1. **Шифрування даних.** Шифрування даних є критично важливим аспектом безпеки хмарних інфраструктур. Шифрування в процесі передачі даних забезпечує захист від перехоплення даних під час їх руху між клієнтом та

хмарними сервісами. Це досягається використанням протоколів, таких як TLS (Transport Layer Security), які забезпечують захищений канал зв'язку. Шифрування даних у стані спокою, з іншого боку, гарантує, що дані залишаються захищеними навіть при фізичному доступі до носіїв інформації. Використання сильних алгоритмів шифрування, таких як AES-256, є стандартною практикою для захисту даних від несанкціонованого доступу.

2. **Багатофакторна аутентифікація (MFA)**. Використання багатофакторної аутентифікації (MFA) значно підвищує рівень безпеки хмарних сервісів. MFA вимагає, щоб користувачі проходили додаткові етапи перевірки, окрім введення пароля. Це може включати використання одноразових паролів (OTP), відбитків пальців або фізичних токенів. Такий підхід суттєво знижує ризик компрометації облікових записів через викрадення або вгадування паролів, забезпечуючи більш надійний захист навіть у випадку, коли пароль стає відомим зловмисникам.
3. **Моніторинг та журналювання**. Постійний моніторинг активності в хмарній інфраструктурі є необхідним для своєчасного виявлення та реагування на підозрілу активність. Це включає ведення журналів усіх дій користувачів, адміністративних змін та системних подій. Журнали дозволяють аналізувати дії після інцидентів, виявляти аномальні патерни поведінки та забезпечувати доказову базу для розслідування. Впровадження систем виявлення вторгнень (IDS) та систем запобігання вторгненням (IPS) дозволяє виявляти та блокувати атаки в режимі реального часу.
4. **Захист від DDoS атак**. Атаки типу "відмова в обслуговуванні" (DDoS) можуть серйозно порушити роботу хмарних сервісів, призводячи до недоступності ресурсів для легітимних користувачів. Для захисту від таких атак використовуються спеціалізовані рішення, що включають мережеві екранування, балансування навантаження та автоматичне виявлення аномальних трафіків. Хмарні провайдери зазвичай надають вбудовані

інструменти для захисту від DDoS, що дозволяють автоматично масштабувати ресурси та блокувати шкідливий трафік.

5. **Ізоляція та віртуалізація**. Забезпечення ізоляції між різними орендарями хмарних ресурсів є критично важливим для запобігання доступу до даних або ресурсів інших клієнтів. Використання безпечних гіпервізорів та технологій віртуалізації дозволяє створити ізольовані середовища для кожного клієнта. Це гарантує, що навіть у випадку компрометації однієї віртуальної машини, інші залишаються захищеними. Крім того, розподіл фізичних та віртуальних ресурсів дозволяє оптимізувати використання інфраструктури, підвищуючи її ефективність та безпеку.
6. **Регулярні оновлення та патчі**. Вразливості у програмному забезпеченні є однією з основних причин компрометації систем. Регулярне оновлення та патчинг програмного забезпечення є необхідним для усунення відомих вразливостей. Хмарні провайдери часто надають автоматичні оновлення безпеки, що дозволяють зменшити ризики, пов'язані з використанням застарілих версій ПЗ. Адміністратори також повинні забезпечувати своєчасне застосування патчів для всіх компонентів інфраструктури, включаючи операційні системи, додатки та мережеві пристрої.
7. **Відповідність стандартам та регуляціям**. Дотримання міжнародних стандартів безпеки, таких як ISO/IEC 27001, SOC 2, та регуляторних вимог, таких як GDPR та HIPAA, є обов'язковим для багатьох організацій. Хмарні провайдери повинні забезпечувати відповідність цим стандартам, надаючи відповідні сертифікати та звіти про аудит. Це дозволяє клієнтам бути впевненими у надійності та безпеці своїх даних. Впровадження політик безпеки, що відповідають регуляторним вимогам, допомагає мінімізувати юридичні ризики та забезпечувати належний захист інформації.
8. **Управління інцидентами безпеки**. Ефективне управління інцидентами безпеки включає розробку планів реагування на інциденти, проведення тренувань та навчань, а також створення команд для швидкого реагування на інциденти. Плани реагування повинні включати процедури для

виявлення, аналізу, усунення та відновлення після інцидентів. Важливо також забезпечити регулярне тестування цих планів для виявлення та усунення можливих недоліків, що дозволяє зменшити час на реагування та мінімізувати вплив інцидентів на бізнес.

9. **Фізична безпека**. Захист фізичних дата-центрів є важливим аспектом забезпечення безпеки хмарних інфраструктур. Це включає контроль доступу до будівель та приміщень за допомогою біометричних сканерів, карт доступу, систем відеоспостереження та охорони. Крім того, важливим є забезпечення надійного резервного живлення, систем пожежогасіння та моніторингу умов середовища (температура, вологість). Це допомагає запобігти фізичним атакам та забезпечити безперервну роботу обладнання в умовах надзвичайних ситуацій.
10. **Управління вразливостями**. Регулярне проведення сканувань на вразливості та тестування на проникнення є необхідними для виявлення потенційних загроз. Інструменти для управління вразливостями допомагають автоматизувати процеси виявлення та усунення вразливостей, забезпечуючи своєчасне застосування патчів та оновлень. Це включає використання автоматизованих сканерів, проведення ручних перевірок та постійне оновлення баз знань про нові загрози. Ефективне управління вразливостями допомагає мінімізувати ризики та забезпечити високий рівень безпеки хмарних інфраструктур.

Дотримання цих вимог дозволяє забезпечити надійний захист хмарних інфраструктур та сервісів, мінімізуючи ризики компрометації даних та забезпечуючи безперебійну роботу бізнесу.

Висновки до розділу 1

У цьому розділі кваліфікаційної роботи було розглянуто ключові аспекти хмарної інфраструктури та сервісів. Визначення понять дозволило чітко окреслити об'єкт дослідження, включаючи різноманітність видів та призначення

хмарних рішень. Дослідження проблем безпеки виявило потенційні ризики та виклики, з якими можуть зіткнутися користувачі хмарних сервісів, та було окреслено сучасні вимоги до безпеки хмарних інфраструктур та сервісів. Загалом, розділ підкреслює значущість ретельного вибору постачальників хмарних сервісів та необхідність комплексного підходу до забезпечення безпеки даних у хмарі.

Хмарна інфраструктура та сервіси відіграють ключову роль у сучасному цифровому світі, надаючи гнучкість та масштабованість для бізнесу та особистих потреб. Вони дозволяють користувачам використовувати обчислювальні ресурси, зберігання даних та програмне забезпечення через Інтернет, не володіючи фізичним обладнанням. Хмарні сервіси поділяються на кілька основних категорій: Інфраструктура як сервіс (IaaS), Платформа як сервіс (PaaS), Програмне забезпечення як сервіс (SaaS), хмарні зберігальні системи та хмарні послуги обробки даних.

Однак, з розвитком хмарних технологій з'являються нові вразливості та виклики для безпеки. Поширені помилки включають відсутність багатофакторної автентифікації, повну довіру хмарному постачальнику, відсутність резервного копіювання, ігнорування регулярних виправлень та неправильну конфігурацію хмари. Ці вразливості можуть призвести до витоку даних, інфікування шкідливим програмним забезпеченням та інших загроз для інформаційної безпеки.

Сучасні вимоги до безпеки хмарних інфраструктур та сервісів включають заходи, описані в оновленому стандарті ISO/IEC 27001:2022, який включає контроль за інформаційною безпекою при використанні хмарних сервісів. Важливо враховувати договірні аспекти безпеки та забезпечувати систематичне визначення процесів придбання, використання, управління та виходу з хмарних сервісів. Компанії повинні також інвестувати в додаткові засоби контролю безпеки, щоб забезпечити захист даних та відповідність нормам і стандартам.

У підсумку, хмарні інфраструктури та сервіси пропонують значні переваги, але також вимагають ретельного підходу до безпеки, щоб мінімізувати ризики та захистити важливі дані.

Розділ 2. ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ ТЕСТУВАННЯ ЗАХИЩЕННОСТІ ХМАРНИХ ІНФРАСТРУКТУР ТА СЕРВІСІВ

2.1 Мета та особливості тестування захищеності хмарних інфраструктур та сервісів.

Тестування захищеності хмарних інфраструктур та сервісів є ключовим аспектом забезпечення інформаційної безпеки в сучасному цифровому світі. Цей процес включає в себе ряд методів і підходів, які дозволяють оцінити стійкість систем до потенційних загроз і вразливостей. Серед таких методів можна виділити сканування вразливостей, пентестування, аналіз вразливостей, Red teaming та соціально-інженерне тестування. Кожен з цих методів має свої особливості та призначений для виявлення певних типів вразливостей.

Сканування вразливостей дозволяє швидко ідентифікувати відомі слабкі місця в системі, використовуючи бази даних вразливостей. Пентестування, або проникнення, включає активні дії з моделювання атак на систему для перевірки її здатності протистояти реальним загрозам. Аналіз вразливостей передбачає глибоке дослідження системи на предмет потенційних слабкостей, які можуть бути використані зловмисниками. Red teaming - це комплексний підхід, який включає в себе створення сценаріїв атак та їх виконання командою експертів з метою виявлення слабких місць. Соціально-інженерне тестування фокусується на людському факторі, виявляючи вразливості, пов'язані з можливістю маніпулювання персоналом або користувачами системи.

Мета тестування захищеності полягає не лише в ідентифікації вразливостей, але й у розробці рекомендацій щодо їх усунення та підвищення загального рівня безпеки. Особливості тестування включають в себе адаптацію методів під конкретні умови експлуатації хмарних сервісів, врахування специфіки хмарних технологій та потреб користувачів. Важливим аспектом є також розуміння правового поля, в якому функціонують хмарні сервіси, адже воно може впливати на вибір методів тестування та інтерпретацію результатів.

Вивчення сучасних методів тестування захищеності вимагає постійного оновлення знань, оскільки технології розвиваються, а з ними з'являються нові загрози та вразливості. Тому професіонали в галузі інформаційної безпеки повинні бути готові до навчання та адаптації своїх навичок під змінювані умови. З огляду на це, роль тестування захищеності стає ще більш значущою, адже воно дозволяє не тільки виявляти слабкі місця, але й прогнозувати потенційні ризики, що сприяє створенню більш надійних та безпечних хмарних сервісів.

Одною з особливостей тестування захищеності хмарних середовищ є необхідність врахування специфічних аспектів хмарних технологій, таких як мультиорендарність, динамічне масштабування ресурсів та інтеграція різних хмарних сервісів. Тестування включає проведення різних видів перевірок, таких як вразливість сканування, тестування на проникнення, аудит конфігурацій та перевірка безпеки API. Оскільки хмарні інфраструктури часто містять складні та взаємопов'язані компоненти, важливо забезпечити комплексний підхід до тестування, включаючи як автоматизовані інструменти, так і ручні перевірки. Регулярне тестування дозволяє виявити нові вразливості, які можуть з'явитися з оновленнями програмного забезпечення або змінами конфігурацій, та своєчасно їх усунути, забезпечуючи тим самим високий рівень безпеки та надійності хмарних сервісів.

Основні етапи проведення тестування на проникнення хмарного середовища включають:

Рис. 2.1. Етапи проведення тестування на проникнення [20]

Планування та підготовка. На цьому етапі визначаються цілі та обсяг тестування. Команда тестувальників разом з керівництвом організації обговорює, які системи та мережі будуть тестуватися, методи, які будуть використовуватися, і які обмеження та правила слід дотримуватися. Крім того, визначаються юридичні аспекти, такі як отримання необхідних дозволів та погоджень на проведення тестування. Цей етап також включає складання графіку проведення тестування та визначення контактних осіб для комунікації під час тестування.

1. ***Розвідка (інформаційний збір).*** Розвідка, або збір інформації, є критичним етапом, де тестувальники збирають якомога більше інформації про цільову систему. Цей процес може бути активним або пасивним. Пасивна розвідка включає аналіз відкритих джерел, таких як публічні вебсайти та соціальні мережі, для збору даних про систему без привернення уваги. Активна розвідка, навпаки, включає взаємодію з цільовими системами для

отримання додаткової інформації, такої як сканування портів, виявлення служб і банерного зняття (banner grabbing).

2. ***Аналіз вразливостей.*** На цьому етапі зібрана інформація аналізується для виявлення потенційних вразливостей. Тестувальники використовують різноманітні інструменти та методи, такі як автоматизовані сканери вразливостей, щоб ідентифікувати слабкі місця в системі. Цей аналіз може виявити проблеми, пов'язані з неправильними налаштуваннями, застарілим програмним забезпеченням, слабкими паролями, відсутністю шифрування та іншими вразливостями, які можуть бути використані зловмисниками.
3. ***Експлуатація вразливостей.*** Після виявлення вразливостей тестувальники намагаються використати їх для проникнення в систему. Цей етап включає спроби отримати несанкціонований доступ до систем, даних або ресурсів, використовуючи методи, подібні до тих, які використовують реальні зловмисники. Мета цього етапу - визначити, чи можуть вразливості бути використані для досягнення цілей атакуючого, таких як крадіжка даних, зміна конфігурацій або виконання шкідливого коду.
4. ***Постексплуатаційний аналіз.*** Після успішного проникнення тестувальники аналізують отримані результати, щоб зрозуміти наслідки експлуатації вразливостей. Це включає оцінку ступеня компрометації системи, впливу на бізнес та потенційних ризиків для організації. На цьому етапі також здійснюється збір доказів та документування всіх дій, що були виконані під час тестування.
5. ***Звітність.*** Результати тестування на проникнення документуються у звіті, який включає детальний опис виявлених вразливостей, методів їх експлуатації та рекомендації щодо їх усунення. Звіт повинен бути чітким та зрозумілим для технічного та керівного персоналу організації. Він включає також оцінку ризиків для бізнесу та пропозиції щодо покращення загальної безпеки системи.

Проведення тестування на проникнення є безперервним процесом, який повинен здійснюватися регулярно, щоб забезпечити постійну безпеку систем та своєчасне виявлення нових вразливостей.

2.2 Аналіз існуючих методологій тестування хмарних інфраструктур та сервісів.

Аналіз методологій тестування на проникнення хмарних інфраструктур та сервісів є ключовим для забезпечення безпеки та надійності цих систем. Враховуючи швидкий розвиток хмарних технологій, важливо розуміти, які методи тестування є найбільш ефективними для виявлення потенційних вразливостей. Традиційні підходи до тестування можуть не бути достатньо адаптованими до динамічної природи хмарних сервісів, де ресурси розподіляються та масштабуються "на льоту". Сучасні методології повинні враховувати ці особливості, а також забезпечувати можливість тестування в різних умовах та конфігураціях [21], [22].

З огляду на це, існують спеціалізовані інструменти та фреймворки, які дозволяють проводити глибокий аналіз безпеки хмарних інфраструктур. Вони включають автоматизовані сканери вразливостей, інструменти для проведення соціальної інженерії, а також системи для симуляції атак на рівні мережі та застосунків. Важливою частиною процесу є також регулярне оновлення баз даних вразливостей та адаптація тестових сценаріїв до новітніх загроз.

Проведення тестування на проникнення в хмарних середовищах вимагає від тестувальників глибокого розуміння хмарної архітектури та використовуваних технологій [23]. Це також передбачає знання про різні моделі розгортання, включаючи публічні, приватні та гібридні хмари, та їхні специфічні ризики. Тестувальники повинні бути знайомі з такими поняттями, як

віртуалізація, контейнеризація, оркестрація, та здатні використовувати інструменти для автоматизації тестування.

Окрім технічних аспектів, ефективне тестування на проникнення також включає розуміння правових та нормативних вимог. Це означає, що тестувальники повинні бути обізнані з відповідними стандартами безпеки, такими як ISO/IEC 27001 [24], NIST [25], та GDPR [26], які можуть впливати на вимоги до безпеки хмарних сервісів. Вони також повинні враховувати політики та процедури, які застосовуються в організації, що використовує хмарні рішення.

Кожна хмарна платформа має свої особливості, але загалом існує кілька основних аспектів, які пентестер повинен перевірити під час проведення тестування на проникнення хмарного середовища [27]:

***Перевірки відповідності стандартам**:*

- **Оцінка розміру середовища та використовуваних сервісів**: Допомагає зрозуміти масштаб хмарної інфраструктури та виявити швидкі помилки конфігурації за допомогою автоматизованих інструментів.
- **Виявлення швидких помилок конфігурації**: Більшість цих перевірок можна виконати автоматизованими засобами, що дозволяє швидко знайти потенційні проблеми.

***Перелічення сервісів**:*

- **Виявлення додаткових помилок конфігурації**: Якщо попередні перевірки були проведені правильно, навряд чи тут знайдеться багато нових проблем, але можна знайти ті, що не були виявлені під час перевірки стандартів.

- **Оцінка використаних сервісів**: Це дозволить точно визначити, які сервіси використовуються у хмарному середовищі, що буде корисним на наступних етапах.

Перевірка відкритих активів:

- **Ідентифікація активів, що можуть бути відкриті для Інтернету**: Під час попереднього етапу необхідно визначити все, що потенційно може бути доступне з Інтернету, та способи доступу до них.
    - **Виявлення вручну відкритих інфраструктурних компонентів**: Включає інстанції з веб-сторінками або відкритими портами, а також інші керовані хмарою сервіси, що можуть бути налаштовані для доступу (наприклад, бази даних або сховища).
- **Оцінка можливості доступу до ресурсів**: Перевірка, чи можуть ці ресурси бути доступні (конфіденційна інформація, вразливості, помилки конфігурації в відкритому сервісі).

Перевірка дозволів:

- **Аналіз дозволів ролей/користувачів у хмарі**: Виявлення всіх дозволів для кожної ролі/користувача та способу їх використання.
    - **Аналіз привілейованих акаунтів**: Чи не забагато акаунтів з високими привілеями? Більшість цих перевірок вже повинні були бути виконані під час оцінки відповідності стандартам.
    - **Оцінка авторизації користувачів**: Якщо клієнт використовує OpenID, SAML або інший спосіб авторизації, потрібно дізнатися додаткову інформацію про те, як призначаються ролі (один користувач або сто користувачів мають роль адміністратора).
- **Виявлення чутливих дозволів**: Необхідно знати не тільки, хто має адміністративні права "*:*", які надають користувачу повний доступ до

системи. Існує багато інших дозволів, які можуть бути дуже чутливими в залежності від використовуваних сервісів.

- **Шляхи підвищення привілеїв**: Слід враховувати потенційні шляхи підвищення привілеїв шляхом зловживання дозволами. Всі можливі шляхи підвищення привілеїв повинні бути задокументовані [28].

***Перевірка інтеграцій**:*

- **Інтеграції з іншими хмарними середовищами або SaaS**: Ймовірно, що всередині хмарного середовища використовуються інтеграції з іншими платформами.
    - **Внутрішньохмарні інтеграції з іншими платформами**: Дізнатися, хто має доступ до використання (або зловживання) інтеграцією, і дізнатися в замовника про легітимність виконуваних дій. **Наприклад**, хто може записувати дані у AWS bucket, з якого GCP отримує дані? (Запитайте, наскільки чутлива дія у GCP, яка обробляє ці дані).
    - **Інтеграції з зовнішніми платформами**: Запитати, хто має зовнішній доступ до використання (або зловживання) інтеграцією і перевірити, як використовуються ці дані. **Наприклад**, якщо сервіс використовує Docker-образ, розміщений у GCR, потрібно запитати, хто має доступ до модифікації цього образу і яку чутливу інформацію та доступ він отримає при виконанні всередині AWS cloud.

Поглиблена методологія:

- **Контрольні перевірки** в хмарній інфраструктурі відіграють вирішальну роль у забезпеченні безперебійної роботи та ефективного управління IT-ресурсами. Вони дозволяють адміністраторам не тільки моніторити поточний стан систем, але й прогнозувати потреби у ресурсах, аналізувати тенденції використання та оптимізувати витрати. Ці перевірки включають в себе оцінку навантаження на сервери, аналіз трафіку мережі, перевірку стану безпеки, а також оцінку ефективності використання хмарних сервісів.

Систематичне проведення контрольних перевірок допомагає виявляти не тільки загальні помилки конфігурації, але й специфічні для хмарних середовищ проблеми, такі як неправильне розподілення ресурсів або надмірне використання послуг, що може призвести до непотрібних витрат. Автоматизація цих процесів за допомогою спеціалізованих інструментів значно знижує ризик людської помилки, підвищує точність перевірок та забезпечує можливість швидкого реагування на виявлені проблеми.

Використання автоматизованих інструментів для контрольних перевірок у хмарній інфраструктурі також сприяє кращому управлінню ліцензуванням програмного забезпечення, оскільки вони дозволяють точно відстежувати використання ліцензій та уникати їх надлишку або нестачі. Це також допомагає у виявленні застарілого або непідтримуваного програмного забезпечення, що може становити ризик для безпеки.

Загалом, контрольні перевірки є невід'ємною частиною стратегічного планування та управління хмарною інфраструктурою, дозволяючи підтримувати високий рівень продуктивності, безпеки та оптимізації ресурсів. Вони є ключовим інструментом для забезпечення сталого розвитку та адаптації до швидко змінних умов сучасного цифрового світу.

- **Перелічування сервісів** є критично важливим етапом у процесі тестування на проникнення, оскільки воно дозволяє виявити всі сервіси, які використовуються в хмарному середовищі. Цей процес включає в себе детальний аналіз конфігурації системи, що допомагає ідентифікувати потенційні слабкі місця та вразливості, які можуть бути недоступні для автоматизованих інструментів. Під час перелічування сервісів фахівці з тестування на проникнення зосереджуються на виявленні та аналізі всіх активних сервісів, їх версій, конфігураційних файлів, використовуваних протоколів та портів.

Крім того, цей етап дозволяє визначити, які саме сервіси використовуються і як вони налаштовані, що є необхідним для планування подальших дій. Наприклад, якщо в ході попередніх контрольних перевірок було встановлено, що всі сервіси налаштовані правильно, то можна зробити висновок про високий рівень безпеки системи. Однак, якщо під час перелічування сервісів виявляються конфігураційні помилки, це може вказувати на потенційні ризики, які потребують негайного виправлення.

Також важливо зазначити, що перелічування сервісів не обмежується лише виявленням активних компонентів. Воно також включає в себе перевірку налаштувань безпеки, аналіз політик доступу, перевірку сертифікатів та інших механізмів шифрування, які використовуються для захисту даних. Це дозволяє отримати повне уявлення про стан безпеки хмарного середовища та визначити, чи відповідають налаштування вимогам стандартів безпеки.

У підсумку, перелічування сервісів є фундаментальним для розуміння архітектури хмарного середовища та визначення потенційних точок входу для зловмисників. Цей етап допомагає встановити основу для всіх подальших етапів тестування на проникнення, включаючи сканування вразливостей, експлуатацію виявлених слабких місць та розробку стратегій захисту. Тому, важливість перелічування сервісів не можна недооцінювати, оскільки від його якості залежить успіх всього процесу тестування на проникнення.

- **Перевірка вразливих активів** є ключовим елементом управління хмарною інфраструктурою, яка вимагає ретельного підходу та систематичності. Цей процес починається з ідентифікації всіх активів, які можуть бути доступні через Інтернет, включаючи веб-сервери, бази даних, сховища даних, а також інші сервіси та застосунки. Важливо не лише виявити ці активи, але й оцінити рівень їх критичності та потенційний вплив на безпеку хмарної інфраструктури у разі компрометації.

Під час перелічування сервісів, яке часто виконується за допомогою автоматизованих інструментів, необхідно звернути увагу на конфігурацію портів, правила фаєрволу, а також налаштування мережевих протоколів. Це дозволить виявити активи, які були виставлені публічно, чи то навмисно, чи випадково, та оцінити ризики, пов'язані з їх доступністю.

Після того, як активи будуть ідентифіковані, слід провести аналіз на предмет вразливостей. Це включає в себе перевірку на наявність відомих вразливостей, використання інструментів для сканування вразливостей, а також ручний аналіз конфігурацій та логів. Особливу увагу слід приділити активам, які містять конфіденційну інформацію, оскільки вони можуть стати ціллю для кібератак.

Важливо також враховувати, що хмарна інфраструктура є динамічною та постійно змінюється. Тому процес перевірки вразливих активів має бути неперервним та включати регулярні оновлення інвентаризації активів, перегляд правил доступу та налаштувань безпеки. Залучення до цього процесу команди безпеки, адміністраторів систем та розробників дозволить забезпечити більш ефективний захист від потенційних загроз.

- **Перевірка привілеїв у хмарній інфраструктурі** є критично важливою для забезпечення безпеки та дотримання політик доступу. Кожна роль та користувач повинні мати чітко визначені права доступу, які відповідають їхнім функціональним обов'язкам, без надмірних привілеїв, що можуть призвести до ненавмисних помилок або зловмисних дій. Ретельна перевірка привілеїв допомагає виявити занадто привілейовані аккаунти та невикористовувані ключі, які часто стають вразливими точками в системі безпеки.

Під час аудиту безпеки, особливу увагу слід приділити методам автентифікації та авторизації, таким як OpenID чи SAML. Важливо зрозуміти, яким чином ролі та права привласнюються користувачам, і чи існують

процедури для перевірки та коригування цих привілеїв. Недостатньо лише ідентифікувати облікові записи з адміністративними привілеями; необхідно також оцінити інші привілеї, які можуть бути чутливими та надавати значний доступ до хмарних ресурсів.

Крім того, важливо виявити потенційні вектори для підвищення привілеїв, які можуть бути використані для обходу політик безпеки. Це включає в себе аналіз конфігурацій, правил доступу та інших механізмів контролю, які можуть бути експлуатовані. Під час тестування на проникнення, необхідно використовувати ці вектори для визначення можливостей несанкціонованого доступу та впливу на хмарні сервіси. Всі знайдені вектори підвищення привілеїв повинні бути задокументовані та включені до звіту про аудит безпеки, щоб можна було розробити відповідні стратегії мінімізації ризиків.

Забезпечення відповідності привілеїв до необхідного мінімуму, постійний моніторинг та аналіз використання привілеїв, а також регулярне оновлення політик безпеки є ключовими для підтримання надійної хмарної інфраструктури. Використання автоматизованих інструментів для управління ідентичностями та доступом може значно полегшити цей процес, забезпечуючи високий рівень безпеки без надмірного обтяження адміністративного персоналу.

- У сфері хмарних технологій, **інтеграція різних сервісів та платформ** є ключовим аспектом для забезпечення ефективності та гнучкості операцій. Інтеграції можуть включати з'єднання хмарних середовищ з іншими хмарними провайдерами, такими як AWS, Azure, GCP, або з SaaS-продуктами, які надають спеціалізовані послуги, наприклад, CRM-системи, бази даних або аналітичні інструменти. При перевірці інтеграцій важливо визначити, які облікові записи мають дозвіл на доступ до інтегрованих ресурсів, оскільки це може вплинути на безпеку та конфіденційність даних. Наприклад, у випадку інтеграції з AWS, необхідно з'ясувати, хто має право записувати дані в S3 bucket, який може

бути використаний іншими сервісами, такими як GCP, для подальшої обробки.

Крім того, слід розглянути наскільки чутливою є інформація, яка передається між сервісами, та які заходи безпеки застосовуються для захисту цих даних. Це може включати шифрування даних під час передачі та зберігання, а також використання мережевих політик і протоколів доступу для контролю доступу до інформації. Якщо інтеграція включає використання Docker-образів, розміщених у Google Container Registry (GCR), важливо забезпечити, що доступ до модифікації цих образів мають лише авторизовані особи. Також слід враховувати, які конфіденційні дані та рівні доступу будуть надані цим образам при їх запуску в хмарному середовищі, наприклад, AWS.

При аудиті хмарної інфраструктури, особливу увагу слід приділити інтеграціям, які виконуються з зовнішніми платформами. Необхідно з'ясувати, хто має зовнішній доступ до цих інтеграцій та яким чином використовуються дані, які передаються через ці інтеграції. Це може включати перевірку політик безпеки, контроль доступу та аудит логів для виявлення будь-яких незвичайних або несанкціонованих дій. Також важливо забезпечити, що всі інтеграції відповідають встановленим стандартам безпеки та приватності, а також відповідають вимогам замовника щодо обробки та зберігання даних.

Успішне тестування на проникнення вимагає не тільки технічних знань, але й стратегічного підходу. Тестувальники повинні визначити цілі тестування, розробити план, який включає всі необхідні етапи, від вибору інструментів до аналізу результатів, та встановити критерії успіху. Вони також повинні бути готові до адаптації своїх методів у відповідь на несподівані виклики та зміни в тестовому середовищі.

Завдяки постійному розвитку технологій та зростанню кількості хмарних сервісів, потреба в кваліфікованих фахівцях, які можуть проводити тестування

на проникнення, лише зростає. Це створює можливості для IT-спеціалістів, які прагнуть розвивати свої навички в цій галузі, та підкреслює важливість навчання та сертифікації в області безпеки хмарних обчислень. З огляду на це, існують численні ресурси, курси та сертифікаційні програми, які можуть допомогти фахівцям підвищити свою кваліфікацію та залишатися в курсі останніх тенденцій у сфері хмарної безпеки.

2.3 Аналіз існуючих програмних інструментів та автоматизованих сканерів з метою підвищення ефективності процесу тестування

Аналіз існуючих програмних інструментів та автоматизованих сканерів є ключовим для підвищення ефективності процесу тестування. Використання правильних інструментів може значно збільшити продуктивність тестування, забезпечуючи більш швидке виявлення помилок та дефектів, а також поліпшення якості програмного забезпечення. Автоматизовані сканери дозволяють автоматизувати повторювані тестові випадки, зменшуючи потребу в ручному тестуванні та звільняючи час тестувальників для більш складних завдань.

Тестування програмного забезпечення охоплює різні види та етапи, включаючи модульне, інтеграційне, системне та приймальне тестування. Кожен з цих типів має свої особливості та вимоги до інструментів тестування. Наприклад, модульне тестування фокусується на окремих компонентах програми, тоді як інтеграційне тестування перевіряє взаємодію між різними модулями.

Важливість тестування програмного забезпечення не можна недооцінювати, оскільки воно забезпечує високу якість продукту та його безпеку. Помилки в програмному забезпеченні можуть призвести до серйозних наслідків, тому ретельне тестування є невід'ємною частиною процесу розробки.

Для ефективного тестування важливо мати чіткий план, який включає визначення цілей тестування, критеріїв прийнятності, тестових сценаріїв та

підготовку даних. Автоматизація тестування може включати використання фреймворків для автоматизованого тестування, інструментів для ручного тестування, засобів для генерації тестових даних та систем контролю версій.

В сучасному світі, де хмарні технології стають все більш поширеними, безпека хмарних інфраструктур та сервісів набуває особливої ваги. Інструменти для оцінки безпеки дозволяють виявляти потенційні вразливості та забезпечувати захист від кібератак. Тестування на проникнення є важливим елементом у цьому процесі, оскільки воно імітує атаки зловмисників та допомагає зрозуміти, як можуть бути експлуатовані слабкі місця системи. Аудит конфігурацій також відіграє ключову роль, оскільки неправильні налаштування можуть відкрити шлях для несанкціонованого доступу.

Використання одного інструменту може не дати повної картини безпеки, тому фахівці рекомендують комбінувати різні методи та інструменти для більш глибокого аналізу. Це може включати статичний аналіз коду, динамічний аналіз, сканування вразливостей, аудит правил брандмауера, перевірку шифрування та багато іншого. Кожен інструмент має свої сильні та слабкі сторони, і їх ефективне поєднання може значно підвищити рівень безпеки хмарних сервісів. Найбільш популярними на даний момент інструментами та сканерами для проведення тестування захищеності хмар є наступні:

1. **Astra Pentest.** Astra Pentest — це хмарний інструмент для автоматизованого і ручного тестування безпеки веб-додатків, мобільних додатків, API та мереж. Він забезпечує комплексний підхід до пентесту, поєднуючи автоматичне сканування з ручним тестуванням експертами з кібербезпеки. Astra Pentest проводить повне сканування для виявлення вразливостей, генерує детальні звіти з рекомендаціями щодо усунення проблем і інтегрується з DevOps інструментами та платформами, такими як Jira і Slack. Це хмарне рішення допомагає відповідати стандартам безпеки та регуляторним вимогам, таким як GDPR та ISO 27001.

Незважаючи на високу вартість для малих компаній і залежність від інтернету, Astra Pentest пропонує всебічний захист і підтримку експертів для ефективного управління безпекою.

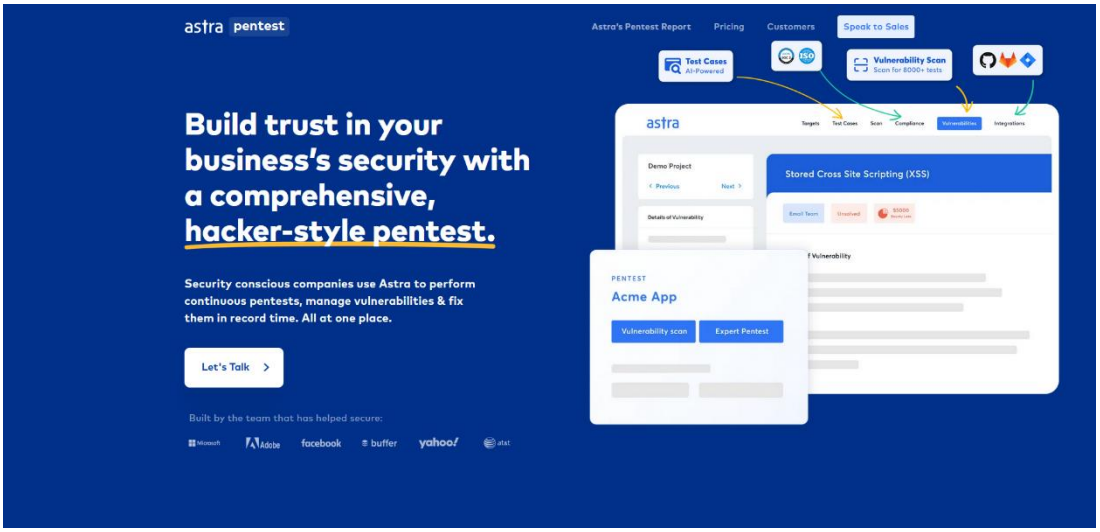

Рис. 2.2. Платформа Astra для проведення автоматизованих сканувань та тестувань на проникнення [29]

2. **Intruder.** Intruder Cloud Scanning — це хмарний інструмент для автоматизованого сканування безпеки, який виявляє вразливості в веб-додатках, мережах та інфраструктурі. Інструмент проводить регулярне сканування систем для виявлення потенційних загроз, забезпечуючи своєчасне оновлення та усунення проблем. Intruder Cloud Scanning генерує детальні звіти про знайдені вразливості та надає рекомендації щодо їх виправлення, допомагаючи організаціям дотримуватися стандартів безпеки, таких як GDPR і ISO 27001. Інтеграція з DevOps інструментами та платформами управління проєктами, такими як Jira, забезпечує безперервний моніторинг і швидке реагування на загрози. Незважаючи на те, що рішення може бути дорогим для малих компаній і залежить від стабільного інтернет-з'єднання, Intruder Cloud Scanning пропонує потужний захист та постійну підтримку для ефективного управління безпекою.

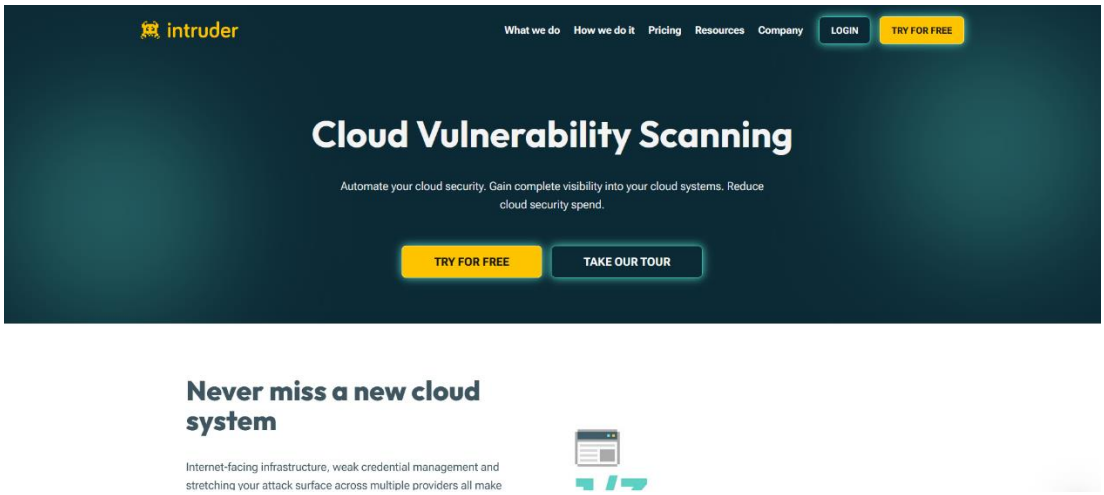

Рис. 2.3. Платформа Intruder для проведення автоматизованих сканувань [30]

3. Nessus. Nessus — це популярний інструмент для автоматизованого сканування вразливостей, розроблений для виявлення та усунення потенційних загроз у веб-додатках, мережах та інфраструктурі. Він проводить детальне сканування систем для виявлення відомих вразливостей, конфігураційних помилок і шкідливих програм. Nessus генерує докладні звіти з інформацією про виявлені проблеми та надає рекомендації щодо їх усунення, допомагаючи організаціям відповідати стандартам безпеки, таким як PCI DSS і HIPAA. Інструмент легко інтегрується з різними системами управління безпекою та платформами для управління інцидентами. Незважаючи на вартість ліцензії та потребу у кваліфікованих спеціалістах для оптимального використання, Nessus забезпечує високий рівень захисту завдяки своєму потужному функціоналу та регулярним оновленням бази вразливостей.

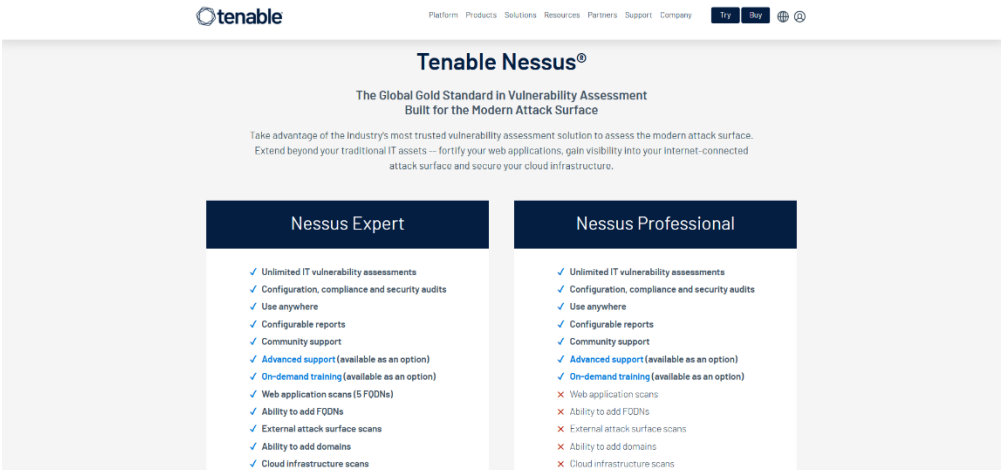

Рис. 2.4. Автоматизований сканер Nessus для проведення сканувань на вразливості [31]

4. Scout Suite. CloudSuite — це хмарний інструмент для комплексного управління безпекою та забезпечення відповідності стандартам. Він пропонує автоматизоване сканування вразливостей у веб-додатках, мережах і хмарних інфраструктурах, виявляючи потенційні загрози та конфігураційні помилки. CloudSuite генерує детальні звіти про знайдені вразливості та надає рекомендації щодо їх усунення, допомагаючи організаціям дотримуватися регуляторних вимог, таких як GDPR та ISO 27001. Інструмент інтегрується з DevOps платформами та системами управління проєктами для забезпечення безперервного моніторингу безпеки. Хоча вартість CloudSuite може бути високою для невеликих компаній, і він залежить від стабільного інтернет-з'єднання, цей інструмент пропонує потужний захист та підтримку експертів для ефективного управління безпекою у хмарних середовищах.

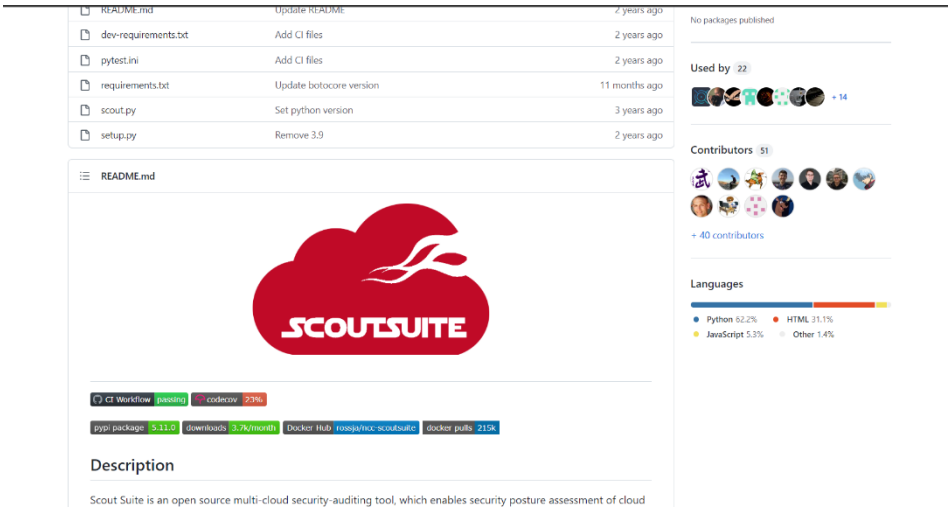

Рис. 2.5. Інструмент з відкритим вихідним кодом ScoutSuite для проведення оцінки безпеки хмар [32]

5. Pacu. Pacu — це спеціалізований інструмент для тестування безпеки хмарної інфраструктури Amazon Web Services (AWS). Він розроблений для виявлення вразливостей і оцінки безпеки конфігурацій AWS. Pacu дозволяє користувачам автоматизувати різні тести безпеки, імітувати атаки та виявляти потенційні загрози у хмарних середовищах. Інструмент надає детальні звіти про знайдені проблеми та рекомендації щодо їх усунення, допомагаючи забезпечити відповідність стандартам безпеки, таким як CIS AWS Foundations Benchmark. Завдяки своїй спеціалізації на AWS, Pacu інтегрується з іншими інструментами та сервісами AWS для забезпечення безперервного моніторингу та захисту. Незважаючи на те, що використання Pacu вимагає певних технічних знань та досвіду роботи з AWS, він забезпечує потужний і цілеспрямований захист хмарної інфраструктури, роблячи його цінним інструментом для організацій, що використовують AWS.

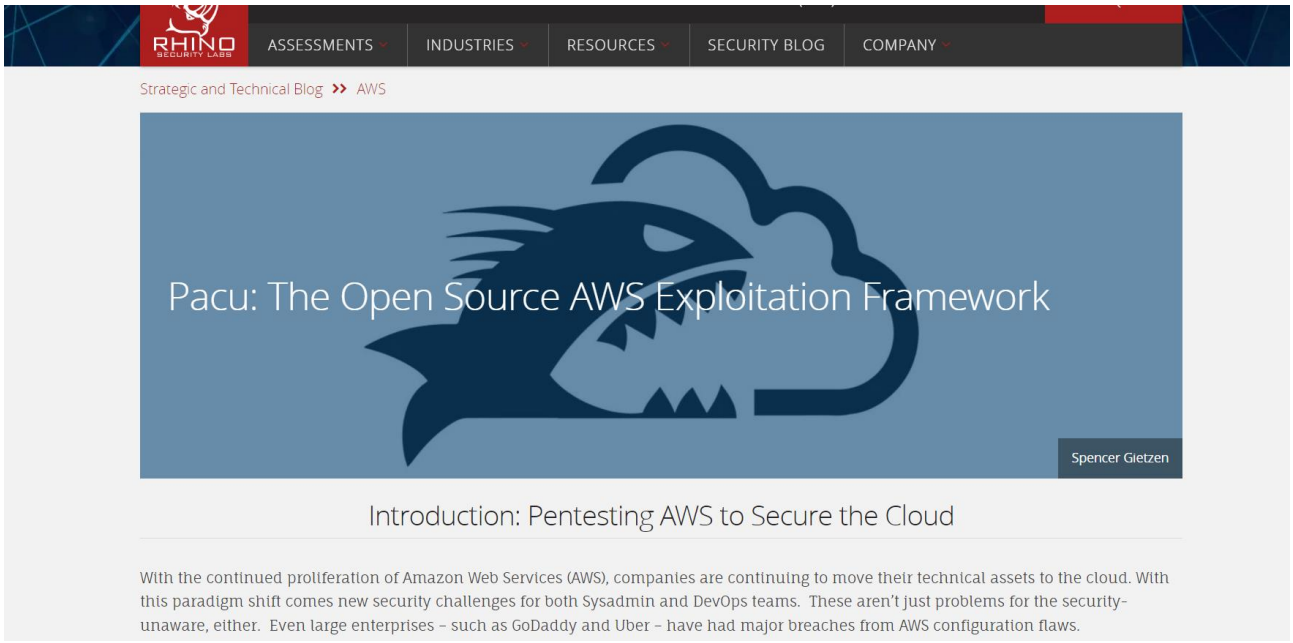

Рис. 2.6. Фреймворк з відкритим вихідним кодом Pacu для проведення оцінки безпеки хмар [33]

6. Nmap. Nmap — це популярний і потужний інструмент для мережевого сканування та аудиту безпеки. Він призначений для виявлення хостів і служб у мережі, а також для визначення їхніх характеристик і конфігурацій. Nmap використовує різноманітні техніки сканування, щоб ідентифікувати відкриті порти, виявити активні служби, визначити операційні системи і навіть виявити можливі вразливості. Інструмент генерує детальні звіти, які допомагають адміністраторам мережі розуміти стан безпеки та приймати відповідні заходи для її покращення. Завдяки своїй гнучкості та широкому функціоналу, Nmap може використовуватися як для невеликих мереж, так і для великих корпоративних інфраструктур. Хоча Nmap є потужним і безкоштовним інструментом, його ефективне використання вимагає певних технічних знань і досвіду в галузі мережевої безпеки.

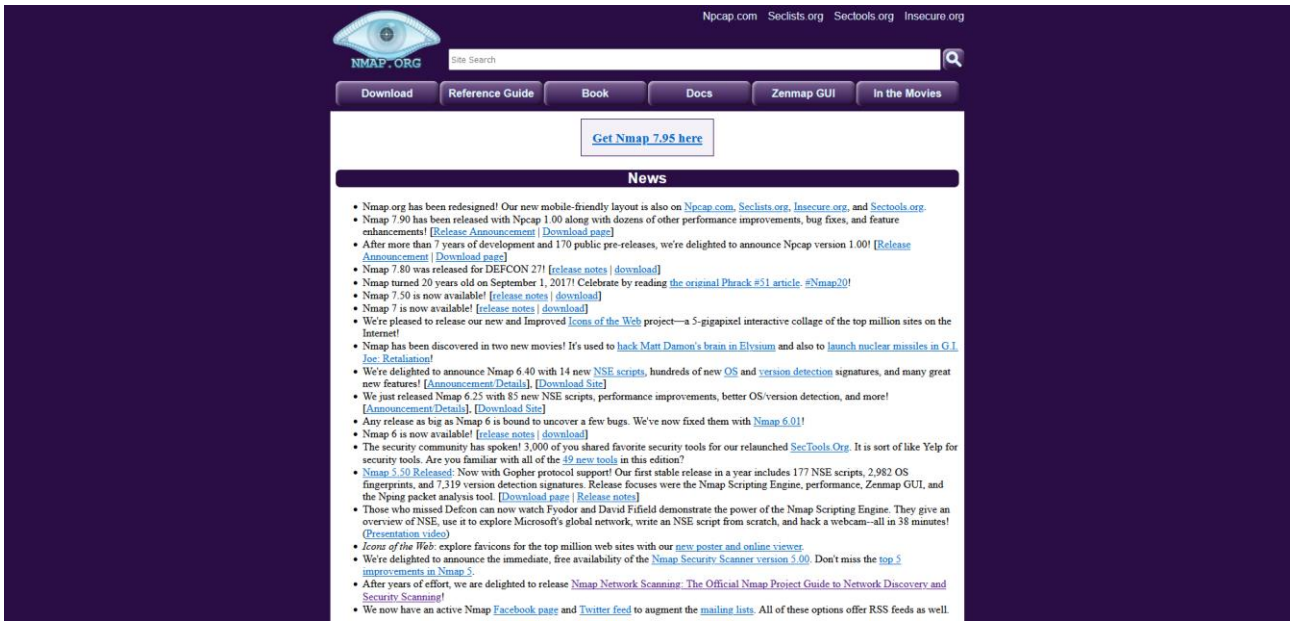

Рис. 2.7. Утиліта з відкритим вихідним кодом NMAP для проведення мережевих сканувань [34]

7. AWS Inspector. AWS Inspector — це хмарний інструмент від Amazon Web Services, призначений для автоматизованої оцінки безпеки та відповідності в AWS середовищах. Він аналізує робочі навантаження AWS, щоб виявити вразливості, неправильні конфігурації та потенційні загрози. AWS Inspector проводить ретельне сканування інфраструктури, включаючи аналіз мережевих конфігурацій і тестування безпеки встановлених додатків. Інструмент генерує детальні звіти з оцінкою ризиків і рекомендаціями щодо усунення виявлених проблем, допомагаючи організаціям дотримуватися стандартів безпеки, таких як PCI DSS і CIS AWS Foundations Benchmark. Завдяки інтеграції з іншими AWS сервісами, такими як AWS CloudTrail і AWS Config, AWS Inspector забезпечує безперервний моніторинг та швидке реагування на загрози. Хоча використання AWS Inspector може вимагати певних знань AWS інфраструктури, він пропонує потужний інструментарій для покращення безпеки та відповідності у хмарних середовищах.

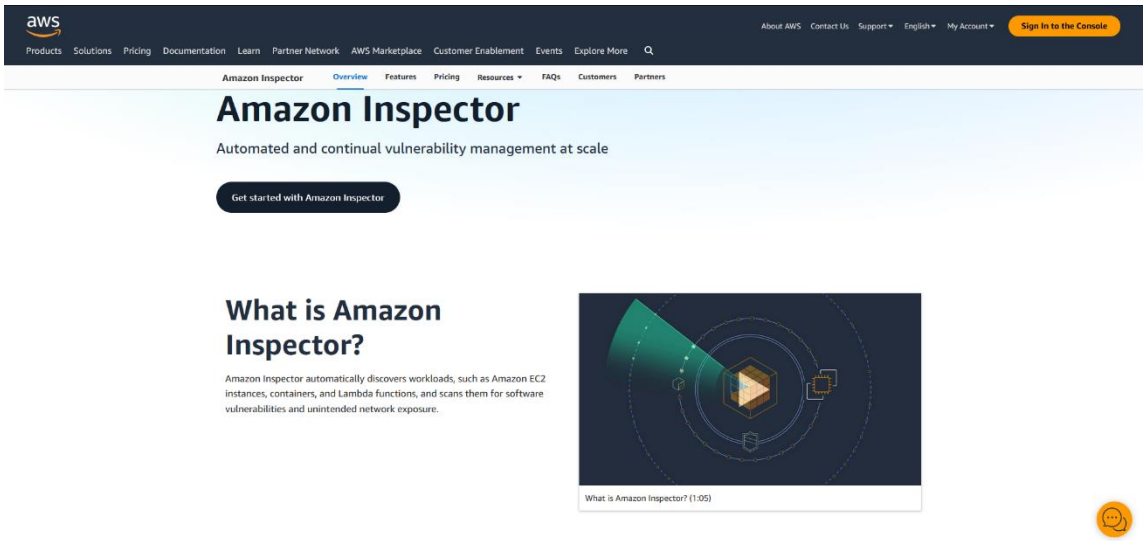

Рис. 2.8. Автоматизований сканер AWS Inspector для проведення комплексної оцінки безпеки хмарних середовищ AWS [35]

8. CloudBrute. CloudBrute — це інструмент для виявлення ресурсів у хмарних інфраструктурах, призначений для тестування безпеки. Він автоматично сканує хмарні платформи, такі як AWS, Google Cloud, та Azure, для виявлення піддоменів, сховищ, серверів та інших хмарних активів. CloudBrute допомагає виявляти неправильно налаштовані ресурси, що можуть бути вразливими до атак. Інструмент генерує звіти про знайдені ресурси та можливі загрози, надаючи рекомендації щодо їх усунення. Завдяки своїй здатності швидко і ефективно виявляти хмарні активи, CloudBrute є корисним для організацій, що прагнуть покращити видимість та безпеку своїх хмарних інфраструктур. Хоча інструмент є потужним і ефективним, його використання вимагає певних знань у галузі хмарних технологій і безпеки.

Рис. 2.9. Утиліта з відкритим вихідним кодом CloudBrute для проведення розвідки під час тестування захищеності [36]

9. MicroBurst. MicroBurst — це інструмент для тестування безпеки хмарних середовищ, зокрема Azure. Він призначений для автоматизованого виявлення вразливостей та неправильно налаштованих ресурсів у хмарній інфраструктурі. MicroBurst використовує різноманітні скрипти та модулі для аналізу конфігурацій, пошуку прихованих ресурсів, перевірки політик безпеки та оцінки загроз. Інструмент генерує детальні звіти з інформацією про знайдені вразливості та рекомендаціями щодо їх усунення. Завдяки своїй спеціалізації на Azure, MicroBurst допомагає організаціям ефективно захищати свої хмарні ресурси та відповідати стандартам безпеки. Хоча його використання вимагає певних знань про Azure та безпеку хмарних інфраструктур, MicroBurst забезпечує потужний і цілеспрямований захист для користувачів платформи Azure.

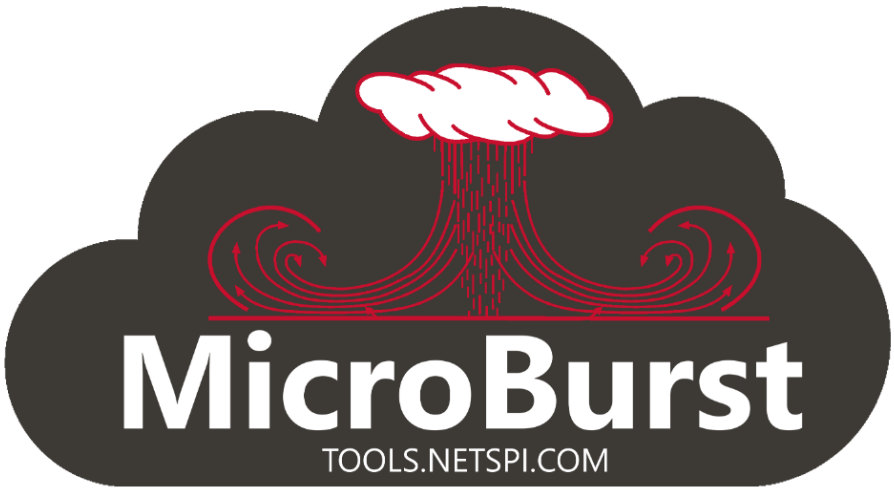

Рис. 2.10. Утиліта з відкритим вихідним кодом MicroBurst для проведення оцінки безпеки хмар [37]

Важливо розуміти, що жоден інструмент не може гарантувати 100% безпеку, але систематичне та ретельне використання набору інструментів може значно знизити ризики. Крім того, важливою є регулярна оцінка та оновлення інструментів, оскільки кіберзагрози постійно еволюціонують. Також корисною є співпраця з професіоналами в області кібербезпеки, які можуть допомогти налаштувати інструменти та інтерпретувати результати тестувань для виявлення та усунення потенційних загроз. Завдяки цьому підходу, організації можуть забезпечити більш надійний захист своїх хмарних інфраструктур та сервісів.

Висновки до розділу 2

У цьому розділі було розглянуто мету та ключові особливості тестування захищеності хмарних інфраструктур та сервісів, що є важливим для забезпечення безпеки даних та послуг. Аналіз існуючих методологій показав, що хоча вже розроблено багато підходів до тестування, існує потреба у їх постійному оновленні та адаптації до змінюваних умов хмарних технологій. Аналіз програмних інструментів та автоматизованих сканерів показав, що використання розглянутих інструментів може значно підвищити ефективність процесу тестування, забезпечуючи більш швидке виявлення та усунення потенційних вразливостей. Втім, автоматизовані інструменти не зможуть повноцінно замінити оцінку безпеки шляхом тестування на проникнення.

Отже, для підвищення ефективності тестування захищеності хмарних інфраструктур та сервісів необхідно інтегрувати сучасні програмні інструменти та автоматизовані системи, а також регулярно оновлювати методологічні підходи, враховуючи новітні розробки в галузі хмарних технологій.

Розділ 3. РОЗРОБКА РЕКОМЕНДАЦІЙ ДЛЯ ТЕСТУВАННЯ ЗАХИЩЕННОСТІ ХМАРНИХ ІНФРАСТРУКТУР ТА СЕРВІСІВ

3.1 Формулювання завдання

Для проведення якісної оцінки безпеки хмарних інфраструктур та сервісів шляхом тестування на проникнення необхідно мати чіткий та послідовний план, відповідний до типу цілі тестування. Наразі немає певної універсальної методології, яка зможе забезпечити повноцінне та якісне проведення тестування захищеності хмар. Тому було вирішено розробити рекомендації для проведення тестувань на проникнення окремо хмарних сервісів та хмарних інфраструктур, які будуть корисними під проведення тестувань. Таким чином, завдання буде виглядати так:

- Розробити рекомендації для тестування на проникнення хмарних інфраструктур та сервісів, які будуть поєднувати у собі вже існуючі етапи тестування, методології, програмні застосунки та утиліти, що в результаті дозволить тестувальникам на проникнення комплексно протестувати всі аспекти хмарного середовища з метою забезпечення конфіденційності, цілісності та доступності інформації користувачів.

Розроблені рекомендації повинні охопити наступні аспекти:

- Етапи тестування на проникнення хмарних інфраструктур та сервісів;
- Способи використання практичних утиліт та сканерів для виявлення вразливостей та помилок у конфігураціях.

3.2 Розробка рекомендацій для тестування захищеності хмарних інфраструктур та сервісів

Не дивлячись на велику кількість існуючих методологій тестування захищеності хмарних середовищ, важливим фактом є той факт, що для проведення тестування на проникнення хмарних інфраструктур та для проведення тестування на проникнення хмарних сервісів необхідні різні програмні інструменти, автоматизовані сканери та методології. Наразі не існує чітких методологій для проведення тестування для кожного з цих напрямків, але загальні етапи пентесту завжди однакові. Проте, зосередити увагу необхідно лише на частині практичних етапів, до яких не входять етапи підготовки та звітності. До них входять:

1. Розвідка (інформаційний збір)
2. Аналіз вразливостей
3. Експлуатація вразливостей
4. Постексплуатаційний аналіз

Кожен з цих етапів вимагає ретельного планування та виконання, а також спеціалізованих інструментів та методик. Тому подальші рекомендації будуть надані в межах окремих етапів для тестування як для хмарних інфраструктур, так і для хмарних сервісів [38], [39], [40], [41].

3.2.1 Розробка рекомендацій для тестування захищеності хмарних інфраструктур

Тестування на проникнення хмарних інфраструктур - це комплексний процес оцінки безпеки всієї хмарної інфраструктури, включаючи всі віртуальні машини, мережі, сховища, бази даних, політики доступу та управління, сервіси, а також будь-які інші ресурси, розгорнуті в хмарі. Основна увага має бути приділена аудиту конфігурацій хмари, а також проведенню мережевих

сканувань. Основними аспектами тестування захищеності хмарних інфраструктур є:

- **Перевірка конфігурацій хмарних ресурсів.** Оцінка безпеки об'єктів сховищ, таких як AWS S3, Google Cloud Storage, Azure Blob Storage, а також аналіз налаштувань безпеки баз даних та інших сервісів [42], [43], [44].
- **Мережеві тести**. Проведення сканування портів, тестування мережевих служб, виявлення відкритих портів та неправильних конфігурацій.
- **Перевірка віртуальних мереж.** Перевірка конфігурацій VPC (Virtual Private Cloud), субмереж, маршрутизації, правил безпеки.

AWS Inspector, наприклад, є спеціалізованим інструментом для інфраструктури AWS, який не підходить для використання в інших хмарних середовищах. З іншого боку, інструменти, такі як CloudBrute та ScoutSuite, фокусуються на аналізі конфігурацій та виявленні неправильних налаштувань, які можуть призвести до вразливостей. Nessus, зі свого боку, є потужним сканером вразливостей, який шукає відомі вразливості та застарілі версії програмного забезпечення, що можуть бути експлуатовані зловмисниками.

Важливо розуміти, що жоден інструмент не може гарантувати 100% виявлення всіх вразливостей, тому рекомендується використовувати комбінацію різних інструментів та методів для всебічної оцінки безпеки. Крім того, важливо регулярно оновлювати інструменти та методики оцінки, щоб вони відповідали найновішим загрозам та тенденціям у сфері кібербезпеки. Такий підхід дозволяє створити більш надійну та ефективну систему захисту хмарних середовищ.

Застосування цих кроків та рекомендацій дозволить ефективно ідентифікувати вразливості в хмарних інфраструктурах та розробити стратегії для їх усунення, зменшуючи ризик кібератак та забезпечуючи вищий рівень безпеки.

Керуючись цими аспектами та особливостями хмарних інфраструктур, тестувальник на проникнення повинен послідовно дотримуватись усіх етапів тестування:

Етап «Розвідка». Розвідка є критично важливим етапом у процесі тестування на проникнення, оскільки саме на цьому етапі збирається інформація, яка буде використовуватися для подальших дій. Під час розвідки, тестувальники зосереджуються на зборі даних про цільову систему, що включає визначення конфігурацій хмарних сервісів, прав доступу користувачів, а також виконання мережевих сканувань для виявлення відкритих портів та активних сервісів. Це дозволяє виявити потенційні слабкі місця та вразливості, які можуть бути використані для проникнення в систему. Для ефективного збору інформації рекомендується використовувати різноманітні інструменти та ресурси. Пошукові системи та онлайн-платформи можуть бути корисними для знаходження загальнодоступної інформації про ціль. Дорки (пошукові запити для виявлення інформації, яка не повинна бути публічною) можуть допомогти виявити вразливі точки. Бази даних вразливостей можуть надати інформацію про відомі слабкі місця в системах та програмному забезпеченні, які можуть бути присутні в цільовій інфраструктурі. Ось деякі рекомендації для виконання етапу розвідки:

1. Визначити обсяг тестування: Чітко визначте, які компоненти хмарної інфраструктури підлягають тестуванню, включаючи мережеві сегменти, системи, додатки та інші активи.
2. Збір інформації: Використовувати відкриті джерела та інші методи для збору інформації про цільову інфраструктуру. Звернути увагу на будь-яку інформацію, яка може бути використана для планування атак.
3. Аналіз отриманої інформації: Оцінити зібрані дані, щоб визначити потенційні слабкі місця та вектори атак.

4. Планування атак: На основі аналізу розробити стратегію тестування, визначивши, які інструменти та техніки будуть використовуватися для виявлення вразливостей.

Етап «Оцінка вразливостей». Оцінка вразливостей є ключовим компонентом процесу оцінки безпеки хмарних середовищ. Цей етап дозволяє виявити потенційні слабкі місця, які можуть бути використані для зловмисних цілей. Використання автоматизованих інструментів значно спрощує та прискорює процес виявлення вразливостей, однак важливо вибирати правильні інструменти, які відповідають специфіці конкретного хмарного середовища. Рекомендації для виконання аналізу вразливостей:

1. Використання перевірених інструментів: Обрати надійні та актуальні інструменти для сканування, які регулярно оновлюються та підтримуються.
2. Комплексний підхід: Комбінувати автоматизоване сканування з ручним аналізом для всебічного виявлення вразливостей.
3. Навчання та розвиток команди: Забезпечити постійне навчання та розвиток навичок команди, щоб вони могли ефективно використовувати інструменти та методики аналізу.
4. Регулярність перевірок: Проводити аналіз вразливостей регулярно, щоб вчасно виявляти нові потенційні загрози.
5. Врахування нових загроз: Слідкувати за останніми дослідженнями в області безпеки та оперативно включати інформацію про нові вразливості у процес аналізу.

Етап «Експлуатація вразливостей». Етап експлуатації вразливостей безпосередньо залежить від успіху попередніх етапів - збору інформації та оцінки вразливостей. На цьому етапі, тестувальник використовує зібрані дані для ідентифікації та використання слабких місць у системі з метою перевірки захисту трьох ключових аспектів інформації: її конфіденційності, цілісності та

доступності. Управління вразливостями вимагає ретельного планування та виконання, а також постійного моніторингу та оновлення, щоб забезпечити захист від нових та еволюціонуючих загроз.

Для ефективної експлуатації вразливостей рекомендується використовувати спеціалізовані інструменти та техніки, які дозволяють автоматизувати процес виявлення та використання слабких місць у захисті хмарних сервісів. Серед таких інструментів можуть бути AWS Inspector, Amazon GuardDuty, AWS Config, які спеціально розроблені для роботи з хмарними сервісами AWS. Також важливо враховувати, що хмарні сервіси постійно оновлюються та змінюються, тому інструменти для тестування мають бути гнучкими та адаптованими до динаміки хмарного середовища.

Під час експлуатації вразливостей необхідно дотримуватися принципу мінімального втручання, щоб звести до мінімуму можливість завдання шкоди інфраструктурі та забезпечити, щоб тестування не впливало на доступність сервісів для інших користувачів. Крім того, важливо враховувати політику хмарного провайдера щодо тестування на проникнення, оскільки деякі дії можуть бути заборонені або вимагати попереднього схвалення.тРекомендації для ефективної експлуатації вразливостей включають:

1. Ретельний вибір інструментів та методів тестування, які відповідають специфіці хмарної інфраструктури.
2. Постійне оновлення баз знань про вразливості та методи їх експлуатації.
3. Використання автоматизованих сканерів вразливостей для швидкого виявлення потенційних слабких місць.
4. Дотримання етичних норм та законодавства під час проведення тестування.

Завдяки дотриманню цих рекомендацій, можна не тільки ефективно виявити та експлуатувати вразливості, але й забезпечити високий рівень безпеки хмарних інфраструктур.

Етап «Постексплуатаційний аналіз». Постексплуатаційний аналіз є кінцевим етапом активних дій у процесі тестування на проникнення хмарних інфраструктур. Цей етап включає детальний розгляд даних, зібраних під час експлуатації вразливостей, з метою ідентифікації та аналізу слідів атаки, виявлення додаткових вразливостей, які не були виявлені на попередніх етапах, та розробки рекомендацій щодо посилення безпеки системи. Для ефективного постексплуатаційного аналізу рекомендується:

1. Документування всіх дій та змін: Зберігайте повний журнал всіх дій, виконаних під час експлуатації вразливостей, включаючи команди, запити та відповіді сервера.
2. Аналіз логів: Перегляньте логи системи та застосунків, щоб виявити аномалії та підозрілу поведінку, яка могла бути пропущена під час активної фази тестування.
3. Використання спеціалізованих інструментів: Застосуйте інструменти для аналізу вразливостей та інцидентів, які можуть допомогти виявити складні аномалії та забезпечити глибший аналіз безпеки.
4. Оцінка впливу: Визначте, який вплив могли мати виявлені вразливості на безпеку хмарної інфраструктури та дані користувачів.

Застосування цих рекомендацій дозволить не тільки виявити максимальну кількість існуючих вразливостей, але й підвищити загальний рівень безпеки хмарної інфраструктури. Важливо пам'ятати, що постійне вдосконалення процесів безпеки та регулярне тестування є ключовими для захисту від постійно еволюціонуючих кіберзагроз.

3.2.2 Розробка рекомендацій для тестування захищеності хмарних сервісів

Тестування на проникнення хмарних сервісів - це процес оцінки безпеки конкретних хмарних додатків та сервісів, розгорнутих на платформах SaaS (Software as a Service), PaaS (Platform as a Service) або функціональних сервісах, таких як AWS Lambda, Google Cloud Functions тощо [45].

Тестування захищеності хмарних сервісів є важливим для захисту чутливих даних, дотримання регуляторних вимог, таких як GDPR, HIPAA та PCI DSS, та запобігання витокам інформації. Воно допомагає виявити та усунути вразливості, забезпечуючи безпеку даних і систем. Крім того, тестування покращує надійність та стабільність хмарних сервісів, підвищуючи довіру клієнтів та користувачів. Завдяки регулярному тестуванню можна своєчасно виявляти нові загрози та адаптуватися до них, що є критично важливим у сучасному динамічному кіберсередовищі.

Основними аспектами, які необхідно врахувати при проведенні тестувань захищеності різних хмарних сервісів є наступні

- **Додатки як послуга (SaaS):**
  - Тестування безпеки веб-додатків та API, розгорнутих у хмарі.
  - Оцінка автентифікації та авторизації користувачів, захисту даних, логіки додатків.
- **Платформи як послуга (PaaS):**
  - Перевірка безпеки середовищ розробки та розгортання додатків.
  - Аналіз конфігурацій служб баз даних, середовищ виконання та інших сервісів PaaS.
- **Функція як послуга (FaaS):**
  - Оцінка безпеки безсерверних функцій, таких як AWS Lambda або Google Cloud Functions.
  - Аналіз налаштувань середовищ виконання функцій, правил тригерів та інтеграцій з іншими сервісами.

- **Інтеграції та API:**
    - Перевірка безпеки інтеграцій між хмарними сервісами та зовнішніми системами.
    - Тестування захисту API, автентифікації, контролю доступу та обробки даних.

За допомогою представлених аспектів тестувальнику буде легше виконувати процес тестування на проникнення та орієнтуватися на кожному з етапів проведення тестування. Також варто враховувати рекомендації для кожного з цих етапів:

Етап «Розвідка (інформаційний збір)»:

1. Використовувати інструменти для збору інформації, такі як Shodan, Censys або Google Dorks.
2. Перевіряти інформацію про SSL сертифікати, що може надати важливі дані про конфігурацію сервера.
3. Використовувати сканування портів для визначення відкритих портів та запущених служб.
4. Збирати інформацію про DNS, включаючи записи MX та SPF, які можуть вказувати на конфігурацію поштових серверів.
5. Використовувати соціальну інженерію для збору даних від співробітників компанії, але тільки у разі домовленості з замовником.

Важливо пам'ятати, розвідка повинна проводитися в рамках закону та етичних норм. Всі зібрані дані повинні бути використані виключно для визначення вразливостей з метою їх подальшого усунення та підвищення рівня безпеки хмарних сервісів.

Етап «Аналіз вразливостей»:

1. Збір інформації: Перед початком аналізу необхідно зібрати всю доступну інформацію про хмарну інфраструктуру, включаючи деталі конфігурації, використовувані технології та програмне забезпечення.

2. Визначення області тестування: Чітко визначити, які компоненти системи будуть перевірятися на вразливості, щоб зосередитися на найбільш критичних елементах.
3. Використання автоматизованих інструментів: Застосування спеціалізованих інструментів для сканування вразливостей може допомогти виявити відомі слабкі місця та недоліки конфігурації.
4. Ручний аналіз: Після автоматизованого сканування важливо провести ручний огляд результатів, щоб виявити помилки, які могли бути пропущені автоматичними інструментами.
5. Оцінка ризиків: Кожну виявлену вразливість необхідно оцінити з точки зору потенційного впливу на систему та ймовірності її експлуатації.
6. Документування: Всі виявлені вразливості та результати аналізу повинні бути детально задокументовані для подальшого використання при усуненні вразливостей.

Необхідно мати на увазі, що аналіз вразливостей повинен проводитися регулярно, оскільки нові вразливості можуть з'являтися з часом, а старі можуть бути усунені. Також важливо враховувати специфіку хмарних сервісів, таку як масштабованість та динамічність середовища, що може впливати на вразливості системи.

Етап «Експлуатація вразливостей»:

1. Використовувати комплексний підхід, який включає в себе розуміння архітектури хмарної інфраструктури та специфіки хмарних сервісів.
2. Застосовувати автоматизовані інструменти для виявлення та експлуатації вразливостей, такі як AWS Inspector, Amazon GuardDuty, та AWS Config.
3. Проводити тестування відповідно до методології "білого ящика", яка передбачає повне розуміння внутрішньої структури тестованої системи.
4. Враховувати спільну відповідальність з провайдером хмарних сервісів за безпеку, що включає в себе розуміння та дотримання політик та обмежень, встановлених провайдером.

Етап «Експлуатація вразливостей»:

1. Перед початком тестування отримати дозвіл від провайдера хмарних сервісів, оскільки не всі види тестувань дозволені та можуть вимагати попереднього узгодження.
2. Зосередитися на вразливостях, які можуть бути експлуатовані в реальних умовах, та використовувати сценарії атак, які максимально наближені до потенційних загроз.
3. Використовувати етичні підходи та засоби, уникаючи дій, які можуть призвести до реальної шкоди інфраструктурі або втрати даних.
4. Після виявлення та експлуатації вразливостей, негайно повідомити про них провайдера хмарних сервісів для вжиття заходів щодо їх усунення.

Етап «Постексплуатаційний аналіз»:

Постексплуатаційний аналіз є критично важливим етапом у процесі тестування на проникнення, оскільки він дозволяє зрозуміти, які дані могли бути доступні зловмисникам у разі успішної атаки, та визначити, які системи були компрометовані. Рекомендації для ефективного виконання постексплуатаційного аналізу:

1. Збір даних: Зібрати всю інформацію, отриману під час тестування, включаючи логи, скріншоти, та інші докази експлуатації.
2. Аналіз даних: Вивчити зібрані дані, щоб визначити, які системи були зламані, які дані були доступні, та які дії були виконані на компрометованих системах.
3. Оцінка ризиків: Оцінити потенційний вплив виявлених вразливостей на бізнес, включаючи можливість витоку конфіденційної інформації та втрату даних.
4. Розробка плану відновлення: Сформулювати рекомендації щодо усунення виявлених вразливостей та відновлення компрометованих систем.
5. Підготовка звіту: Підготувати детальний звіт, який включає опис виявлених проблем, оцінку ризиків, та рекомендації щодо їх усунення.

Виконання цих рекомендацій допоможе забезпечити, що після тестування на проникнення хмарні сервіси будуть більш захищені та стійкі до майбутніх атак.

Висновки до розділу 3

У цьому розділі було виконано завдання розробки рекомендацій для проведення якісного тестування на проникнення хмарних інфраструктур та сервісів. Ці рекомендації базуються на вже відомих етапах тестування, методологіях, програмних застосунках та утилітах, що дозволяють тестувальникам на проникнення комплексно протестувати всі аспекти хмари з метою забезпечення конфіденційності, цілісності та доступності даних.

Розроблені рекомендації охоплюють етапи тестування на проникнення хмарних інфраструктур, хмарних сервісів, базові методи тестування на проникнення, а також способи використання практичних утиліт та сканерів для виявлення вразливостей. Це дає можливість тестувальникам систематично і послідовно проводити тестування, використовуючи найкращі практики.

Загалом, рекомендації, розроблені у цьому розділі, спрямовані на підвищення рівня безпеки хмарних інфраструктур та сервісів, що є актуальним у контексті зростаючої популярності хмарних технологій та збільшення кількості кібератак. Виконання цих рекомендацій дозволить ефективно ідентифікувати потенційні загрози та своєчасно реагувати на них, забезпечуючи надійний захист інформації.

ВИСНОВКИ

Хмарні інфраструктури та сервіси відіграють ключову роль у сучасному світі, забезпечуючи основу для багатьох технологічних інновацій і бізнес-процесів. Вони надають компаніям гнучкість, масштабованість і економічну ефективність, дозволяючи швидко адаптуватися до змін і запускати нові проєкти без значних капітальних витрат. Хмарні сервіси також сприяють глобальній доступності даних і додатків, забезпечуючи безперебійний доступ до інформації з будь-якої точки світу. Це, в свою чергу, підвищує продуктивність і співпрацю між командами, сприяючи інноваціям і розвитку. Завдяки хмарним технологіям, малі та середні підприємства отримали доступ до потужних обчислювальних ресурсів, які раніше були доступні лише великим корпораціям, що сприяє рівним умовам для бізнесу будь-якого масштабу.

Проте, незважаючи на всі переваги, хмарні середовища також мають свої вразливості та проблеми безпеки, якими не можна нехтувати. Досягти високого рівня захищеності хмарних інфраструктур та сервісів можна лише за допомогою використання найкращих практик безпеки, а також за допомогою регулярних тестувань на захищеність.

У кваліфікаційній роботі було розглянуто ключові аспекти хмарних інфраструктур та сервісів, включаючи їх визначення, види, призначення та поширені вразливості. Було встановлено, що безпека хмарних інфраструктур та сервісів є критично важливою, і сучасні вимоги до безпеки повинні бути виконані для забезпечення захисту даних та послуг. Аналіз сучасних методів тестування показав, що існуючі методології та програмні інструменти можуть бути використані для підвищення ефективності процесу тестування, але також потребують постійного оновлення та адаптації до нових загроз.

У результаті дослідження були розроблені рекомендації для тестування захищеності хмарних інфраструктур та сервісів, як вказують на необхідність інтеграції комплексного підходу, який включає регулярне оновлення безпекових протоколів, використання автоматизованих сканерів для виявлення вразливостей та навчання персоналу для ефективного реагування на інциденти безпеки.

Враховуючи швидкий розвиток технологій та зміну характеру кіберзагроз, рекомендації повинні бути гнучкими та адаптованими до специфіки кожної організації.

У підсумку, для забезпечення надійної захищеності хмарних інфраструктур та сервісів, необхідно постійно вдосконалювати методи тестування та розробляти адаптивні стратегії безпеки, які відповідають сучасним вимогам та викликам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. SP 800-145, The NIST Definition of Cloud Computing | CSRC. *NIST Computer Security Resource Center | CSRC*. URL: https://csrc.nist.gov/pubs/sp/800/145/final (date of access: 31.05.2024).
2. From On-Premise Software to Cloud Services: The Impact of Cloud Computing on Enterprise Software Vendors' Business Models. *SciELO - Scientific electronic library online*. URL: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-18762013000300004&lng=en&nrm=iso&tlng=en (дата звернення: 31.05.2024).
3. What is Cloud Infrastructure? - Definition | VMware Glossary. *VMware*. URL: https://www.vmware.com/topics/glossary/content/cloud-infrastructure.html (дата звернення: 31.05.2024).
4. What is Cloud Infrastructure? Exploring the Power of Cloud Solutions. *SIM-Networks – Your Goals, our Tech. IT Infrastructure from German Provider*. URL: https://www.sim-networks.com/en/blog/cloud-infrastructure (дата звернення: 31.05.2024).
5. Difference Between Public, Private, and Hybrid Cloud. *LogicMonitor*. URL: https://www.logicmonitor.com/blog/difference-between-public-private-and-hybrid-cloud (дата звернення: 31.05.2024).
6. Differentiating Cloud Deployment Models. *Learn SAP skills | SAP Learning*. URL: https://learning.sap.com/learning-journeys/explore-sap-cloud-erp/differentiating-cloud-deployment-models_a58ccb24-3a43-42e0-b58f-2ac5c06e33d6 (дата звернення: 31.05.2024).
7. Cloud Deployment Models - GeeksforGeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/cloud-deployment-models/ (дата звернення: 31.05.2024).
8. URL: https://www.hpe.com/emea_europe/en/what-is/cloud-services.html (дата звернення: 31.05.2024).

9. What are the different types of cloud computing? | Google Cloud. *Google Cloud*. URL: https://cloud.google.com/discover/types-of-cloud-computing (дата звернення: 31.05.2024).
10. Types of Cloud Computing - SaaS vs PaaS vs IaaS - AWS. *Amazon Web Services, Inc.* URL: https://aws.amazon.com/types-of-cloud-computing/ (дата звернення: 31.05.2024).
11. Types of cloud computing. *Red Hat - We make open source technologies for the enterprise*. URL: https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud (дата звернення: 31.05.2024).
12. Модель secaas (security-as-a-service) безпека як послуга набирає популярності - ITPRO.UA. *ITPRO*. URL: https://itpro.ua/post/model_secaas_security_as_a_service_bezopasnost_kak_usluga_nabiraet_populyarnost (дата звернення: 31.05.2024).
13. Cloud deployment models - geeksforgeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/cloud-deployment-models/ (дата звернення: 31.05.2024).
14. OWASP Cloud-Native Application Security Top 10 | OWASP Foundation. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: https://owasp.org/www-project-cloud-native-application-security-top-10/ (дата звернення: 31.05.2024).
15. 8 All-Too-Common Cloud Vulnerabilities | Wiz. *wiz.io*. URL: https://www.wiz.io/academy/common-cloud-vulnerabilities (дата звернення: 31.05.2024).
16. ISO/IEC 27001:2022. URL: https://my-itspecialist.com/iso-iec-27001-2022-standard (дата звернення: 31.05.2024).
17. Про захист персональних даних. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 31.05.2024).
18. Постанова Правлінням Національного банку України від 08 березня 2022 року № 42 "Про використання банками хмарних послуг в умовах воєнного

стану в Україні". *Національний банк України*. URL: https://bank.gov.ua/ua/legislation/Resolution_08032022_42 (дата звернення: 31.05.2024).

19. 11 Cloud Security Best Practices & Tips in 2024. *eSecurity Planet*. URL: https://www.esecurityplanet.com/cloud/cloud-security-best-practices/ (дата звернення: 31.05.2024).
20. 6 Steps to a Penetration Test. *SecurityMetrics*. URL: https://www.securitymetrics.com/blog/6-steps-penetration-test (дата звернення: 31.05.2024).
21. Cloud Penetration Testing: A Complete Guide. *Astra Security Blog*. URL: https://www.getastra.com/blog/security-audit/cloud-penetration-testing/ (дата звернення: 31.05.2024).
22. Cloud Penetration Testing. URL: https://www.guidepointsecurity.com/education-center/cloud-penetration-testing/ (дата звернення: 31.05.2024).
23. Cloud Penetration Testing: Strategies for Success in 2024. *Software Testing Company | Luxe Quality*. URL: https://luxequality.com/blog/cloud-penetration-testing/ (дата звернення: 31.05.2024).
24. ISO/IEC 27001:2022 Compliance - Amazon Web Services (AWS). *Amazon Web Services, Inc.* URL: https://aws.amazon.com/compliance/iso-27001-faqs/?nc1=h_ls (дата звернення: 31.05.2024).
25. National Institute of Standards and Technology. *NIST*. URL: https://www.nist.gov/ (дата звернення: 31.05.2024).
26. GDPR – це Європейський Регламент щодо захисту персональних даних. Суть та штрафи за GDPR. *Legal IT group*. URL: https://legalitgroup.com/gdpr-novi-eu-tendentsii/ (дата звернення: 31.05.2024).
27. Pentesting Cloud Methodology | Ukranian - Ht Cloud | HackTricks Cloud. *HackTricks Cloud | HackTricks Cloud | HackTricks Cloud*. URL: https://cloud.hacktricks.xyz/v/ua-cloud/pentesting-cloud/pentesting-cloud-methodology (дата звернення: 31.05.2024).

28. GCP - Privilege Escalation | Ukranian - Ht Cloud | HackTricks Cloud. *HackTricks Cloud | HackTricks Cloud | HackTricks Cloud*. URL: https://cloud.hacktricks.xyz/v/ua-cloud/pentesting-cloud/gcp-security/gcp-privilege-escalation (дата звернення: 31.05.2024).
29. Hacker-Style Pentest by Astra Security. *Astra Security - Continuous Pentest Platform*. URL: https://www.getastra.com/pentest (дата звернення: 31.05.2024).
30. Cloud Vulnerability Scanner: Automate Security Across the Cloud. *Intruder | Vulnerability Management Made Easy*. URL: https://www.intruder.io/cloud-vulnerability-scanning-for-aws-google-cloud-and-azure (дата звернення: 31.05.2024).
31. Nessus Vulnerability Scanner: Network Security Solution. *Tenable®*. URL: https://www.tenable.com/products/nessus (дата звернення: 31.05.2024).
32. GitHub - nccgroup/ScoutSuite: Multi-Cloud Security Auditing Tool. *GitHub*. URL: https://github.com/nccgroup/ScoutSuite (дата звернення: 31.05.2024).
33. Pacu: The Open Source AWS Exploitation Framework - Rhino Security Labs. *Rhino Security Labs*. URL: https://rhinosecuritylabs.com/aws/pacu-open-source-aws-exploitation-framework/ (дата звернення: 31.05.2024).
34. Nmap: the Network Mapper - Free Security Scanner. *Nmap: the Network Mapper - Free Security Scanner*. URL: https://nmap.org/ (дата звернення: 31.05.2024).
35. Automated Vulnerability Management - Amazon Inspector - AWS. *Amazon Web Services, Inc.* URL: https://aws.amazon.com/inspector/?nc1=h_ls (дата звернення: 31.05.2024).
36. GitHub - 0xsha/CloudBrute: Awesome cloud enumerator. *GitHub*. URL: https://github.com/0xsha/CloudBrute (дата звернення: 31.05.2024).
37. GitHub - NetSPI/MicroBurst: A collection of scripts for assessing Microsoft Azure security. *GitHub*. URL: https://github.com/NetSPI/MicroBurst (дата звернення: 31.05.2024).
38. Reconnaissance - Penetration Testing - GeeksforGeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/reconnaissance-penetration-testing/ (дата звернення: 31.05.2024).

39. Vulnerability Assessment & Penetration Testing | Veracode. *Veracode*. URL: https://www.veracode.com/security/vulnerability-assessment-and-penetration-testing (дата звернення: 31.05.2024).
40. Exploitation in Penetration Testing. *Vertex Cyber Security*. URL: https://www.vertexcybersecurity.com.au/exploitation-in-penetration-testing/ (дата звернення: 31.05.2024).
41. Post-exploitation in penetration testing. *Vertex Cyber Security*. URL: https://www.vertexcybersecurity.com.au/post-exploitation-in-penetration-testing/ (дата звернення: 31.05.2024).
42. Amazon S3 - Cloud Object Storage - AWS. *Amazon Web Services, Inc.* URL: https://aws.amazon.com/s3/?nc1=h_ls (дата звернення: 31.05.2024).
43. Cloud Storage. *Google Cloud*. URL: https://cloud.google.com/storage?hl=en (дата звернення: 31.05.2024).
44. Microsoft Azure Storage Blobs. URL: https://azure.microsoft.com/en-us/products/storage/blobs (дата звернення: 31.05.2024).
45. Cloud Services. *Corporate Finance Institute*. URL: https://corporatefinanceinstitute.com/resources/data-science/cloud-services/ (дата звернення: 31.05.2024).