КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.793
УДК 004.8

Журавчак Анастасія Юріївна
аспірант, асистент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-8196-7963
anastasiia.y.tolkachova@lpnu.ua

Піскозуб Андріян Збігнєвич
кандидат технічних наук, доцент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-3582-2835
andriian.z.piskozub@lpnu.ua

Банах Роман Ігорович
доктор філософії, старший викладач кафедри безпеки інформаційних технологій
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0001-6897-8206
roman.i.banakh@lpnu.ua

Журавчак Даниїл Юрійович
доктор філософії, асистент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0003-4989-0203
danyil.y.zhuravchak@lpnu.ua

Глущенко Павло Костянтинович
аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-1262-5484
pavlo.k.hlushchenko@lpnu.ua

АНАЛІЗ ІНСТРУМЕНТУ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ У ХМАРНИХ ТЕХНОЛОГІЯХ

Анотація. У статті проведено огляд можливостей та архітектури інструменту Scout Suite, який є одним із провідних рішень з відкритим кодом для аудиту безпеки хмарної інфраструктури. Scout Suite розроблений для автоматизованого аналізу конфігурацій хмарних облікових записів з метою виявлення потенційних вразливостей, неправильних налаштувань доступу, відсутності шифрування, слабких політик IAM тощо. Основною перевагою інструменту є мультихмарна підтримка, зокрема для Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), а також в альфа-версіях — Alibaba Cloud та Oracle Cloud Infrastructure. У роботі розглянуто архітектуру інструменту, яка побудована за модульним принципом і складається з основного ядра (Core), модулів для обробки CLI-запитів, інтерфейсів виводу (Output) та окремих компонентів для кожного хмарного провайдера. Завдяки використанню фасадного патерну, Scout Suite дозволяє гнучко розширювати підтримку нових сервісів, при цьому зберігаючи єдину логіку доступу до ресурсів. Інструмент забезпечує збереження результатів у форматі інтерактивних HTML-звітів, які зручно переглядати офлайн, а також підтримує кастомізацію правил та інтеграцію з CI/CD пайплайнами, наприклад, через Jenkins. Особлива увага приділена використанню інструменту в контексті забезпечення безпеки процесів DevSecOps та дотримання стандартів відповідності. Scout Suite дозволяє швидко отримати повний огляд безпеки хмарної інфраструктури, автоматизувати виявлення критичних помилок та скоротити час на ручну перевірку. У статті також окреслено перспективи подальших досліджень, серед яких інтеграція з SIEM-системами, застосування методів машинного навчання для автоматизації аналізу результатів аудиту, розширення підтримки нових хмарних платформ, а також створення специфічних профілів перевірки для стандартів безпеки. Scout Suite розглядається як важливий інструмент у сучасному арсеналі кібербезпеки для організацій, що активно використовують хмарні сервіси.

Ключові слова: тестування на проникнення; хмарні технології; кібербезпека; автоматизований інструмент.

ВСТУП

Традиційний процес тестування на проникнення відомий своїми значними фінансовими зобов'язаннями та потребою у високому рівні експертизи. Він вимагає мати в штаті або за контрактом спеціалістів, які впродовж певного часу проведуть оцінку стану безпеки. Однак, зростання кількості кіберзагроз та збільшення складності атак створюють нові виклики для забезпечення своєчасного й ефективного захисту. У зв'язку з цим автоматизація пентесту стала пріоритетом для багатьох компаній та організацій [1].

Останнім часом багато компаній мігрують до хмарних сервісів (AWS, GCP та Azure) [2]. У порівнянні з локальними серверами, хмарна інфраструктура буде легкою в налаштуванні, масштабуванні, економічно вигідною та простою в обслуговуванні, оскільки вона відповідає поточним бізнес-вимогам. Окрім цього, використання хмарних технологій стає дедалі популярнішим рішенням для більшості власників вебсайтів. У зв'язку з цим фокус тестування безпеки вебзастосунків поступово зміщується в бік виявлення вразливостей саме в хмарній інфраструктурі, на якій працює усе програмне забезпечення сайту. Кількість неправильних конфігурацій (місконфігурацій) постійно зростає, оскільки хмарні сервіси пропонують широкий спектр функцій і налаштувань [3]. Це, у свою чергу, створює велику кількість потенційних точок атаки, які необхідно перевірити під час тестування. Одним із ефективних рішень для цього є використання автоматизованих інструментів, таких як Scout Suite [4].

Постановка проблеми. З огляду на зростання складності кіберзагроз та масове впровадження хмарних технологій, традиційний підхід до пентесту втрачає ефективність через свою тривалість і високу вартість. У таких умовах виникає потреба в автоматизованих інструментах, здатних оперативно виявляти вразливості в хмарній інфраструктурі, зокрема помилки конфігурації, які стають дедалі частішими.

Аналіз останніх досліджень і публікацій. У сфері забезпечення безпеки хмарної інфраструктури спостерігається зростаючий науковий та практичний інтерес до інструментів автоматизованого виявлення вразливостей. Дослідники зосереджують увагу на оцінці ефективності таких рішень, зокрема їх здатності виявляти неправильні конфігурації, надлишкові дозволи та відхилення від галузевих стандартів.

В роботі [5] надають узагальнений огляд трьох ключових інструментів — Postman, Scout Suite та Burp Suite — і їхнього значення для забезпечення безпеки цифрових систем. Автори підкреслюють важливість автоматизованих рішень у виявленні вразливостей API, хмарної інфраструктури та вебзастосунків. Робота є корисною для початкового ознайомлення з можливостями цих інструментів у рамках комплексної стратегії кіберзахисту. Однак не проаналізовано комплексно всі можливості інстументу Scout Suite.

В роботі [6] акцентується на важливості автоматизації процесів моніторингу та виявлення неправильних конфігурацій у хмарних середовищах, зокрема в Google Cloud Platform (GCP). Автори пропонують інтеграцію інструменту Scout Suite для сканування конфігурацій та використання Splunk для візуалізації даних безпеки, що дозволяє ефективніше відстежувати та реагувати на потенційні загрози. Однак, автори не проаналізували всі можливості інстументу Scout Suite щодо пошуку вразливостей у хмарних технологіях.

В роботі [7] основну увагу приділено підвищенню безпеки процесу безперервної інтеграції та доставки шляхом автоматичного виявлення конфігураційних помилок і

впровадження інструментів безпеки. Одним із ключових інструментів, який було інтегровано, став Scout Suite. Його було налаштовано як частину автоматичного сканування в CI/CD, що дало змогу виявляти помилки безпеки ще до деплою у продакшн.

Метою статті є аналіз автоматизованого інструменту для пошуку вразливостей у середовищах із застосуванням хмарних технологій.

МЕТОДИКА ДОСЛІДЖЕННЯ

Для аналізу взято відкритий проєкт Scout Suite. Проаналізовано його можливості та сильні сторони.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Scout Suite — це потужний мультихмарний інструмент для аудиту безпеки з відкритим кодом, створений фахівцями з безпеки для комплексної оцінки конфігурацій хмарної інфраструктури. Він підтримує основні хмарні платформи, включаючи Amazon Web Services, Microsoft Azure, Google Cloud Platform, а також в альфа-версії Alibaba Cloud і Oracle Cloud Infrastructure. Інструмент використовує API постачальників хмарних послуг для збору метаданих, формуючи візуальний звіт, який дозволяє швидко виявити зони ризику без необхідності перегляду численних сторінок консолі. Після збору даних Scout Suite працює в автономному режимі, що зручно для офлайн-аналізу. Конфігурації класифікуються за рівнями ризику: Good, Warning, Danger, що дозволяє фокусуватися на критичних проблемах. Крім того, користувач може вмикати або вимикати правила відповідно до потреб або створювати власні правила перевірки, що робить інструмент дуже гнучким. Для запуску Scout Suite потрібно [8]:

- Python 3.6+.
- Встановлений AWS CLI.
- Створений програмний користувач з політиками ReadOnlyAccess і SecurityAudit, який дозволяє зчитувати метадані ресурсів.

Інструмент підтримує аудит таких сервісів AWS, як EC2, IAM, S3, Route 53 тощо. Звіт зберігається в локальній папці scoutsuite-report, який можна заархівувати, передати або завантажити у S3 для подальшого аналізу [9]. Scout Suite легко інтегрується з CI/CD [10] пайплайнами, наприклад, через Jenkins, завдяки підтримці shell-скриптів. Це дає змогу запускати автоматизовані перевірки безпеки при кожному деплої і зберігати результати у хмарному сховищі для командного доступу або аудиту. Основні переваги:

- Повний огляд безпеки хмарної інфраструктури з підтримкою кількох провайдерів.
- Автоматизовані перевірки конфігурацій, доступів, журналювання, шифрування тощо.
- Гнучке налаштування правил і параметрів.
- Зрозумілі звіти з поділом ризиків і рекомендаціями.
- Підтримка безперервного моніторингу через CI/CD інтеграцію.
- Відсутність ліцензійних витрат — повністю безкоштовний open-source проєкт.
- Жива спільнота користувачів і розробників.

Scout Suite — це незамінний інструмент для команд, які прагнуть зменшити ризики у своїй хмарній інфраструктурі шляхом автоматизованого аналізу, прозорого звітування та безперервного вдосконалення безпекових практик. Його інтеграція в DevSecOps

процеси дозволяє проактивно реагувати на вразливості до їхнього потрапляння в продакшн [11]. На рис. 1 зображено архітектуру інструменту.

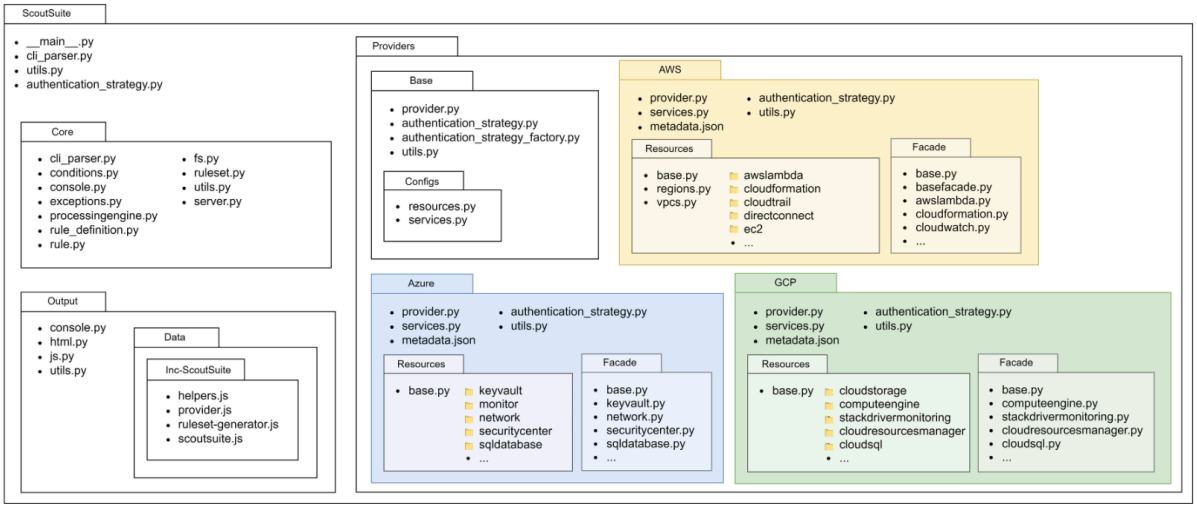

Рис. 1. Огляд архітектури інструменту Scout Suite

Архітектура Scout Suite побудована за модульним принципом, що забезпечує гнучкість, масштабованість і розширюваність інструменту. Основний функціонал зосереджений у кореневій частині, яка містить головні скрипти запуску (__main__.py, cli_parser.py), утиліти (utils.py) та логіку аутентифікації (authentication_strategy.py). Центральна частина інструменту реалізована у модулі Core, що відповідає за обробку командного рядка, визначення та застосування правил аудиту, винятки, логіку обробки даних та взаємодію з файловою системою. Після обробки конфігураційних даних результати виводяться у модулі Output, який генерує звіти у форматах HTML і JavaScript. У папці Inc-ScoutSuite знаходяться JavaScript-файли, які реалізують візуалізацію інтерфейсу перегляду результатів.

Інструмент має чітко сегментовану підтримку хмарних провайдерів. Загальні компоненти знаходяться в модулі Providers, який містить базові скрипти аутентифікації, конфігурації ресурсів і служб. Для кожного провайдера (AWS, Azure, GCP) виділено окремі каталоги з індивідуальними скриптами: для AWS — це підтримка таких сервісів, як EC2, S3, Lambda, VPC, CloudTrail, з відповідними модулями збору метаданих і фасадами для логічного представлення; для Azure — модулі обробки ресурсів, зокрема keyvault, monitor, network, securitycenter, sqldatabase, а також фасадні скрипти для об’єднання логіки; для GCP — підтримка cloudstorage, computeengine, stackdrivermonitoring, cloudsql та відповідні фасади, що забезпечують універсальний доступ до ресурсів.

Особливістю архітектури є застосування фасадного патерну, який дозволяє абстрагуватися від конкретної реалізації ресурсів, зберігаючи при цьому спільну логіку для обробки та візуалізації. Такий підхід спрощує розширення підтримки нових сервісів, а також адаптацію до змін у API провайдерів. Водночас конфігураційна частина підтримує створення власних правил аудиту, що робить Scout Suite не лише інструментом для моніторингу, а й гнучкою платформою для аналізу безпеки у будь-якому хмарному середовищі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Scout Suite є одним із найефективніших інструментів відкритого коду для безпечного

аудиту хмарної інфраструктури, який забезпечує автоматизоване виявлення помилок конфігурації та формування звітів про стан безпеки. Його модульна архітектура, підтримка кількох хмарних провайдерів (AWS, Azure, GCP), гнучкість у налаштуванні правил перевірки та можливість інтеграції з CI/CD пайплайнами робить цей інструмент надзвичайно корисним у практиці DevSecOps. Архітектурна побудова з використанням фасадного патерну дозволяє легко масштабувати функціональність і підтримувати актуальність при оновленні API хмарних сервісів. Подальші дослідження можуть бути спрямовані на глибшу автоматизацію аналізу результатів сканування за допомогою машинного навчання або систем рекомендацій. Перспективним напрямом є також інтеграція Scout Suite з SIEM-платформами для автоматизованої кореляції виявлених вразливостей з подіями безпеки. Окрему увагу заслуговує розширення підтримки нових хмарних провайдерів (наприклад, IBM Cloud або Huawei Cloud), а також створення кастомних ruleset-профілів для конкретних стандартів відповідності (наприклад, CIS Benchmarks або ISO/IEC 27017). Такі дослідження сприятимуть подальшому вдосконаленню інструменту як у напрямку зручності використання, так і в контексті підвищення якості безпеки хмарних середовищ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Piskozub, A., Zhuravchak, D., & Tolkachova, A. (2023). Research on Vulnerabilities in Chatbots Using Large Language Models *Ukrainian Scientific Journal of Information Security*, *29(3),* 111–117. https://doi.org/10.18372/2225-5036.29.18069
2. Borra, P. (2024). An overview of cloud computing and leading cloud service providers. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4914169
3. Singh, B. (2014). Identifying cloud computing vulnerabilities. *International Journal of Scientific Research in Science, Engineering and Technology*, 198–202. https://doi.org/10.32628/ijsrset207250
4. *GitHub - nccgroup/ScoutSuite: Multi-Cloud Security Auditing Tool*. (n. d.). GitHub. https://github.com/nccgroup/ScoutSuite
5. P, A., Sharma, T., Jatain, A., & Bajaj, S. B. (2024). Examining cybersecurity tools for a complete security assessment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4850417
6. Jeya Suriya, B., Amarnath, B. K., Raghuraman, A. R., & Arumugam, C. (2024). Cloud security: Upgradation in CSPM configuration setting. *In 2024 4th international conference on data engineering and communication systems (ICDECS)*. IEEE. https://doi.org/10.1109/icdecs59733.2023.10503211
7. Jackson, L. (2020). The CI/CD pipeline. *In The complete ASP.NET core 3 API tutorial*, 305–347. Apress. https://doi.org/10.1007/978-1-4842-6255-9_12
8. *Setup*. (n. d.). GitHub. https://github.com/nccgroup/ScoutSuite/wiki/Setup
9. *Penetration testing*. (n. d.). Microsoft Learn: Build skills that open doors in your career. https://docs.microsoft.com/en-us/azure/security/azure-security-pen-testing
10. van Merode, H. (2023). CI/CD concepts. *In Continuous integration (CI) and continuous delivery (CD)*, 11–27. Apress. https://doi.org/10.1007/978-1-4842-9228-0_2
11. *Architecture overview*. (n. d.). GitHub. https://github.com/nccgroup/ScoutSuite/wiki/Architecture-overview

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Anastasiia Zhuravchak
Phd student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8196-7963
anastasiia.y.tolkachova@lpnu.ua

Andriian Piskozub
Doctor of Technical Sciences, Associate Professor
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-3582-2835
andriian.z.piskozub@lpnu.ua

Banakh Roman
PhD, Senior Lecturer at the Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0001-6897-8206
roman.i.banakh@lpnu.ua

Danyil Zhuravchak
PhD, Associate Professor
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-4989-0203
danyil.y.zhuravchak@lpnu.ua

Pavlo Hlushchenko
PhD student of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID 0000-0002-1262-5484
pavlo.k.hlushchenko@lpnu.ua

ANALYSIS OF A TOOL FOR DETECTING VULNERABILITIES IN THE CLOUD TECHNOLOGIES

Abstract. This article provides a comprehensive overview of the capabilities and architecture of Scout Suite, one of the leading open-source tools for cloud infrastructure security auditing. Scout Suite is designed for automated analysis of cloud account configurations to identify potential vulnerabilities, misconfigured access controls, missing encryption, weak IAM policies, and more. One of the tool's main advantages is its multi-cloud support, including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), as well as Alibaba Cloud and Oracle Cloud Infrastructure in alpha versions. The study examines the tool's architecture, which follows a modular design and consists of a core engine, CLI request handlers, output interfaces, and dedicated components for each cloud provider. Through the use of the facade pattern, Scout Suite enables flexible support for new services while maintaining a unified logic for accessing resources. The tool generates interactive HTML reports that can be viewed offline and supports both rule customization and integration into CI/CD pipelines, such as via Jenkins. Particular attention is paid to the tool's use in securing DevSecOps processes and achieving compliance with security standards. Scout Suite allows users to gain a full overview of their cloud infrastructure's security posture, automate the detection of critical issues, and significantly reduce the time required for manual review. The article also outlines future research directions, including integration with SIEM systems, the application of machine learning for automated analysis of audit results, expansion to support additional cloud platforms, and the creation of specific verification profiles aligned with security standards. Scout Suite is considered a vital tool in the modern cybersecurity arsenal for organizations that actively rely on cloud services.

Keywords: penetration testing; cloud technologies; cybersecurity; automated tool.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Piskozub, A., Zhuravchak, D., & Tolkachova, A. (2023). Research on Vulnerabilities in Chatbots Using Large Language Models *Ukrainian Scientific Journal of Information Security*, *29(3),* 111–117. https://doi.org/10.18372/2225-5036.29.18069
2. Borra, P. (2024). An overview of cloud computing and leading cloud service providers. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4914169
3. Singh, B. (2014). Identifying cloud computing vulnerabilities. *International Journal of Scientific Research in Science, Engineering and Technology*, 198–202. https://doi.org/10.32628/ijsrset207250
4. *GitHub - nccgroup/ScoutSuite: Multi-Cloud Security Auditing Tool*. (n. d.). GitHub. https://github.com/nccgroup/ScoutSuite
5. P, A., Sharma, T., Jatain, A., & Bajaj, S. B. (2024). Examining cybersecurity tools for a complete security assessment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4850417
6. Jeya Suriya, B., Amarnath, B. K., Raghuraman, A. R., & Arumugam, C. (2024). Cloud security: Upgradation in CSPM configuration setting. *In 2024 4th international conference on data engineering and communication systems (ICDECS)*. IEEE. https://doi.org/10.1109/icdecs59733.2023.10503211
7. Jackson, L. (2020). The CI/CD pipeline. *In The complete ASP.NET core 3 API tutorial*, 305–347. Apress. https://doi.org/10.1007/978-1-4842-6255-9_12
8. *Setup*. (n. d.). GitHub. https://github.com/nccgroup/ScoutSuite/wiki/Setup
9. *Penetration testing*. (n. d.). Microsoft Learn: Build skills that open doors in your career. https://docs.microsoft.com/en-us/azure/security/azure-security-pen-testing
10. van Merode, H. (2023). CI/CD concepts. *In Continuous integration (CI) and continuous delivery (CD)*, 11–27. Apress. https://doi.org/10.1007/978-1-4842-9228-0_2
11. *Architecture overview*. (n. d.). GitHub. https://github.com/nccgroup/ScoutSuite/wiki/Architecture-overview