КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1014
УДК 004.62

Скуратовський Євгеній Олегович
студент кафедри інформаційної та кібернетичної безпеки
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0009-0000-0432-9784
yoskuratovskyi.fitm24m@kubg.edu.ua

Аносов Андрій Олександрович
к.в.н., доцент, доцент кафедри інформаційної та кібернетичної безпеки
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-2973-6033
a.anosov@kubg.edu.ua

Стрельніков Віталій Ігорович
PhD, доцент кафедри інформаційної та кібернетичної безпеки
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0003-3439-3220
v.strelnikov@kubg.edu.ua

Кучерявий Микола Вікторович
аспірант
Інститут проблем математичних машин та систем
Національної академії наук України, Київ, Україна
ORCID: 0009-0005-0017-9797
bu9free@gmail.com

ЕКСПЕРИМЕНТИ ТА ПРАКТИЧНІ РІШЕННЯ ПОБУДОВИ ТЕСТОВОГО СЕРЕДОВИЩА ДЛЯ ПЕРЕВІРКИ РІВНЯ БЕЗПЕКИ НА РІВНІ ДОДАТКІВ

Анотація. У статті розглянуто експериментальні підходи та практичні рішення до побудови тестового середовища для перевірки рівня безпеки на рівні додатків. Метою дослідження є створення ізольованої лабораторної інфраструктури, що імітує структуру корпоративної мережі з DMZ-зоною, внутрішнім сегментом та середовищем атак, для об'єктивної оцінки ефективності сучасних засобів захисту. Тестове середовище реалізовано на базі віртуалізації VMware Workstation Pro з інтеграцією таких інструментів, як Burp Suite Pro, AppScan, ZAP Proxy, Acunetix, Splunk, Wazuh, LogRhythm. Проведено серію експериментів, що включали імітацію типових атак на рівні додатків (SQL-ін'єкція, XSS, CSRF, brute force, мережеве сканування), збір та аналіз логів подій. Результати експериментів показали, що Burp Suite Pro та Splunk мають найвищу комплексну ефективність, тоді як Wazuh і ZAP Proxy забезпечують прийнятну якість при мінімальних витратах ресурсів. Встановлено, що поєднання засобів сканування, моніторингу та реагування в межах багаторівневої моделі безпеки значно підвищує стійкість системи до атак. На основі отриманих даних розроблено практичні рекомендації щодо впровадження комбінованих стратегій захисту на рівні додатків, заснованих на принципах Zero Trust Architecture та DevSecOps. Запропонована модель забезпечує баланс між безпекою й продуктивністю та може бути використана для побудови ефективних систем моніторингу, тестування вразливостей і навчання фахівців з кібербезпеки. Розроблене середовище може бути адаптоване для тестування нових інструментів захисту та моделювання складних сценаріїв атак. Подальші дослідження передбачають удосконалення системи автоматизованого аналізу результатів тестування та розширення функціональності середовища.

Ключові слова: тестове середовище; безпека додатків; Burp Suite; Splunk; Wazuh; DevSecOps; Zero Trust; кіберзагрози.

ВСТУП

Постановка проблеми. У сучасних умовах стрімкого розвитку інформаційних технологій корпоративні інформаційно-комунікаційні системи стають ключовими елементами функціонування підприємств, державних установ і фінансових організацій. Зростання кількості вебдодатків, інтегрованих сервісів та API-інтерфейсів призводить до підвищення ризиків несанкціонованого доступу, втрати конфіденційних даних і компрометації критичних ресурсів. Традиційні засоби захисту, зокрема антивірусне програмне забезпечення та мережеві брандмауери, не забезпечують належного рівня протидії сучасним атакам, спрямованим саме на рівень додатків. Це створює необхідність розроблення ефективних методів аналізу та тестування безпеки програмних систем у контрольованому середовищі, яке дозволяє моделювати реальні сценарії атак і перевіряти дієвість захисних механізмів.

Проблема підвищення рівня безпеки додатків є особливо актуальною для корпоративних структур, які працюють з великими обсягами чутливої інформації. Створення тестового середовища для перевірки рівня захисту на рівні додатків дає змогу проводити експериментальні дослідження, оцінювати ефективність різних методів безпеки, аналізувати їх вплив на продуктивність системи та виробляти практичні рекомендації щодо впровадження оптимальних рішень.

Аналіз останніх досліджень і публікацій. Питання забезпечення безпеки програмних додатків детально висвітлюються у звітах міжнародних організацій, зокрема OWASP [6], NIST [5] та MITRE [4], де визначено ключові принципи виявлення, класифікації та усунення вразливостей у сучасних інформаційних системах. Значний внесок у стандартизацію підходів до аналізу ризиків і побудови систем кіберзахисту зробили ініціативи Cisco [2], які розробили практичні рекомендації для тестування безпеки вебдодатків і мережевої інфраструктури.

У сучасних публікаціях SANS Institute [8] наголошується на важливості інтеграції безпеки у всі етапи життєвого циклу програмного забезпечення, що забезпечує безперервний контроль ризиків і скорочує час реагування на інциденти. Особливу увагу приділено концепції Zero Trust Architecture [12], яка ґрунтується на принципі недовіри до будь-яких суб’єктів або компонентів системи за замовчуванням і передбачає постійне підтвердження автентичності доступу.

Метою статті є висвітлення результатів експериментального дослідження та розроблення практичних рішень для побудови тестового середовища, призначеного для перевірки рівня безпеки на рівні додатків.

Теоретичні основи дослідження базуються на концепціях і методологічних підходах до побудови систем захисту інформації на рівні додатків у корпоративних інформаційно-комунікаційних системах. Основу складає принцип багаторівневого захисту (defense in depth), який передбачає застосування кількох взаємопов’язаних механізмів безпеки для запобігання, виявлення та реагування на інциденти [13-17].

Одним із ключових теоретичних підходів є модель Zero Trust Architecture, згідно з якою жоден компонент системи або користувач не вважається «довіреним» за замовчуванням. Усі запити на доступ до даних перевіряються незалежно від джерела їх походження [12]. Такий підхід забезпечує мінімізацію внутрішніх загроз і несанкціонованих дій у мережі. Реалізація принципів Zero Trust дає змогу підвищити контроль над автентифікацією користувачів, впровадити адаптивне керування доступом і зменшити ризики експлуатації вразливостей.

Другим важливим теоретичним підходом є DevSecOps – інтеграція безпеки в усі етапи життєвого циклу розробки програмного забезпечення. Цей підхід базується на постійній автоматизованій перевірці коду, використанні інструментів статичного (SAST) і динамічного (DAST) аналізу, а також контролі залежностей (Dependency Check, Snyk). Завдяки DevSecOps безпека перестає бути етапом після розробки, стаючи невід'ємною частиною процесу створення продукту [8].

В основу роботи покладено також концепцію CIA triad (Confidentiality, Integrity, Availability) – триєдиної моделі інформаційної безпеки, що визначає конфіденційність, цілісність і доступність даних як базові характеристики захищеної системи. Для підтримання цих характеристик використовуються механізми шифрування, автентифікації, контролю доступу, виявлення вторгнень та моніторингу подій.

Ключовими методами, що застосовуються у системах безпеки на рівні додатків, є:

- шифрування даних для забезпечення конфіденційності під час передачі та зберігання;
- механізми автентифікації та авторизації (зокрема багатофакторна автентифікація – MFA) для підтвердження особи користувачів;
- моніторинг активності з використанням систем SIEM (Splunk, Wazuh, LogRhythm), які дають змогу збирати журнали подій і аналізувати поведінку системи;
- виявлення та запобігання вторгненням (IDS/IPS) для блокування спроб несанкціонованого доступу [10].

Для формалізації оцінки ефективності механізмів захисту в роботі використано низку метрик, серед яких:

- Mean Time to Detect (MTTD) – середній час виявлення інциденту;
- Mean Time to Respond (MTTR) – середній час реагування на інцидент;
- False Positive Rate (FPR) – рівень хибнопозитивних спрацьовувань;
- Patch Management Efficiency – швидкість ліквідації вразливостей через оновлення програмного забезпечення [10].

Таким чином, теоретичне підґрунтя дослідження базується на поєднанні концепцій Zero Trust, DevSecOps, CIA triad, Defense in Depth і сучасних стандартів кібербезпеки (ISO/IEC 27001, NIST, OWASP). Це створює основу для експериментальної перевірки дієвості запропонованих методів захисту на практиці.

Методика дослідження передбачала створення експериментального тестового середовища для перевірки ефективності методів захисту додатків та оцінювання впливу впроваджених рішень на продуктивність системи. Дослідження базувалося на комбінуванні кількісних і якісних методів аналізу.

Тестове середовище реалізовано на платформі VMware Workstation Pro, що дало змогу створити ізольовану інфраструктуру, поділену на три основні сегменти:

- DMZ-зону, де розміщено вебдодатки, що підлягали тестуванню;
- внутрішню корпоративну мережу, що імітувала середовище користувачів і серверів баз даних;
- зовнішнє середовище атак, з якого проводилися імітації вторгнень і перевірка стійкості системи.

У середовищі розгорнуто набір інструментів для сканування вразливостей та аналізу безпеки, серед яких Burp Suite Pro, AppScan, Acunetix, ZAP Proxy, а також системи моніторингу та реагування Splunk, Wazuh, LogRhythm, SolarWinds SEM [1].

Об'єктом дослідження є механізми забезпечення безпеки на рівні додатків у корпоративних IT-системах. А предметом дослідження – методи, технології та

інструменти захисту даних, їх ефективність, інтеграція та вплив на продуктивність системи.

Для оцінки ефективності використано методи:

- кількісний аналіз – розрахунок метрик (MTTD, MTTR, FPR, Patch Management Efficiency);
- порівняльний аналіз – зіставлення ефективності різних інструментів за критеріями точності, інтеграції, продуктивності та зручності;
- моделювання загроз – створення сценаріїв атак типу SQL Injection, XSS, CSRF, brute force тощо;
- статистичний аналіз результатів тестування та журналів SIEM-систем;
- експертне оцінювання – аналіз виявлених вразливостей і реакції систем на атаки.

У процесі оцінювання використовувалися такі критерії:

- точність виявлення загроз;
- рівень хибнопозитивних спрацьовувань;
- можливість інтеграції в CI/CD;
- продуктивність системи;
- масштабованість і зручність використання.

Кожен показник оцінювався у шкалі від 0 до 1 (0 – відсутність функціональності, 1 – повна підтримка), що дозволяло порівняти засоби за сумарною ефективністю.

Етапи проведення дослідження включали:

- розгортання віртуальної інфраструктури;
- інсталяція та налаштування інструментів безпеки;
- імітація типових атак;
- збір логів та метрик SIEM-системами;
- аналіз результатів і формування висновків.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ.

В процесі побудови тестового середовища для перевірки рівня безпеки на рівні додатків та проведення серії експериментів із використанням сучасних інструментів моніторингу, сканування та аналізу вразливостей. Метою експериментальної частини було виявлення ефективних комбінацій засобів безпеки, що забезпечують максимальний рівень захисту при збереженні продуктивності системи.

Архітектура тестового середовища. Тестове середовище побудовано на базі віртуалізації VMware Workstation Pro, що дозволило створити ізольовану інфраструктуру з можливістю контролю трафіку, навантаження та відтворення реальних сценаріїв атак [4]. Архітектура середовища включає три логічно розділені сегменти:

- DMZ-зона (Demilitarized Zone) – зона доступу ззовні, де розміщено вебсервери з тестовими додатками;
- внутрішня корпоративна мережа – сервер баз даних, внутрішній сервер авторизації та SIEM-система;
- середовище атак (Attack Lab) – набір віртуальних машин з Kali Linux, Metasploit, Nmap, Burp Suite Pro та іншими інструментами для моделювання загроз [6].

Завдяки ізоляції кожного сегмента вдалося уникнути перехресного впливу та забезпечити контрольований потік даних між зонами. Компоненти мережі з’єднані за допомогою віртуальних комутаторів, що дозволило моделювати різні конфігурації без втручання у фізичну інфраструктуру [9].

На рисунку 1 зображено загальну архітектуру тестового середовища, де чітко відображено взаємозв'язок між DMZ, внутрішньою мережею та середовищем атак.

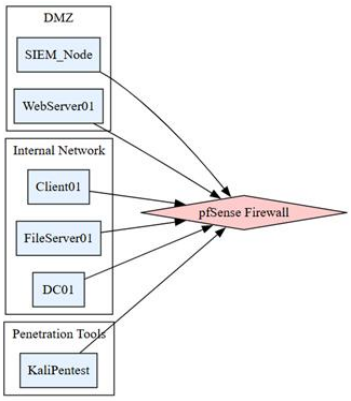

Рис. 3.1 – UML-діаграма топології середовища

Склад і конфігурація середовища. У межах дослідження використано набір інструментів, які розподілено за функціональними групами:

- сканери вразливостей: Burp Suite Pro, AppScan, Acunetix, ZAP Proxy;
- системи моніторингу та реагування (SIEM): Splunk, Wazuh, LogRhythm, SolarWinds SEM;
- інструменти моделювання атак: Metasploit Framework, Nmap, Hydra [7].

Кожен інструмент встановлювався у власному ізольованому контейнері, що дало змогу уникнути конфліктів при одночасному використанні декількох систем. Журнали подій SIEM-систем централізовано зберігалися для подальшого порівняльного аналізу.

Сценарії тестування та типи атак. Для перевірки ефективності засобів захисту було розроблено п'ять основних сценаріїв тестування:

- SQL Injection – моделювання атак на рівні бази даних через маніпуляцію параметрами запитів;
- Cross-Site Scripting (XSS) – вставлення шкідливого JavaScript-коду у форми користувача;
- Cross-Site Request Forgery (CSRF) – виконання запитів від імені користувача без його згоди;
- Brute Force – підбір паролів до систем автентифікації;
- Port Scanning / Reconnaissance – виявлення відкритих портів за допомогою Nmap [3].

Відповідності середовища критеріям оцінки подано в таблиці 1.

Таблиця 1

Відповідності середовища критеріям оцінки

Критерій	**Реалізація у середовищі**
Ізоляція середовища	Повна мережева ізоляція через PfSense (без виходу в Інтернет)
Відтворюваність експериментів	Snapshots + шаблони ВМ
Різноманітність ОС/ролей	Windows, Linux, AD, WebApp, SIEM, Kali
Підтримка активного та пасивного тестування	Всі типи атак і логування забезпечені
Інтеграція захисних засобів	Splunk, Burp, AppScan, ZAP інтегровані та налаштовані
Збір логів/даних	Логування через syslog/SIEM-агенти + ручна валідація

Порівняльний аналіз ефективності сканерів. Аналіз результатів показав, що Burp Suite Pro продемонстрував найвищу точність виявлення вразливостей – 93%, тоді як AppScan – 89%, Acunetix – 85%, а ZAP Proxy – 78%. Водночас частота хибнопозитивних результатів становила відповідно 3%, 5%, 6% і 11%.

Burp Suite відзначився найкращими можливостями кастомізації й інтеграції з CI/CD через Jenkins, що відповідає принципам DevSecOps. AppScan виявився найшвидшим (у середньому 12 хвилин на один цикл сканування), тоді як Acunetix мав найзручніший інтерфейс користувача.

Ефективність систем моніторингу та реагування. У ході дослідження проаналізовано роботу чотирьох SIEM-платформ: Splunk, Wazuh, LogRhythm і SolarWinds SEM. Згідно з експериментальними даними найкращі показники отримано для Splunk – 4,8 бала з 5, що пояснюється високою швидкістю кореляції подій і зручним інтерфейсом керування інцидентами.

Wazuh показав дещо нижчі результати (4,2 бала), однак має перевагу у відкритому коді та гнучкому налаштуванні [11]. LogRhythm і SolarWinds SEM отримали 3,8 та 3,6 бала відповідно через обмежену масштабованість і більшу потребу в ресурсах.

Під час моделювання атаки типу Brute Force було зафіксовано, що Splunk виявляє інцидент через 2 секунди після початку атаки, тоді як Wazuh через 4 секунди, а LogRhythm через 6 секунд.

Комплексна оцінка результатів. Для узагальнення даних було розраховано інтегральний показник ефективності (Ef), який враховує точність виявлення, швидкість реагування та стабільність роботи систем [2]. Результати порівняльного аналізу векторів атак і реакцій систем наведено в таблиці 2.

Таблиця 2.

Порівняльний аналіз ефективності

Вектор атаки	Інструмент атаки	Виявлено засобами захисту	Реакція SIEM / логування
SQLi	sqlmap	AppScan, ZAP Proxy, Burp Suite	Wazuh (MITRE T1190), Splunk (індексована подія)
XSS	Burp Suite	ZAP, AppScan	Виявлення заголовків, логування Reflected-XSS
CSRF	Burp Repeater	Частково (тільки AppScan)	Відсутність захисту – низький рівень ефективності
Brute-force	Hydra	Wazuh, Burp (Intruder)	Alert після >5 спроб автентифікації (MITRE T1110)
SMB Enumeration	enum4linux	—	Логування через auditd, без активації попереджень

Як видно з таблиці 2, найкращі результати продемонстровано під час виявлення атак типу SQLi та XSS, які ефективно фіксувалися як сканерами вразливостей, так і SIEM-системами. Водночас CSRF-атаки виявилися найменш контрольованими, оскільки лише частина інструментів реєструвала їх прояви, а системи моніторингу не формували відповідних попереджень [5].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ.

У результаті проведених експериментів було підтверджено ефективність поєднання сучасних засобів захисту додатків у корпоративному середовищі. Розроблене тестове середовище дало змогу змоделювати реальні сценарії атак, зокрема SQL-ін’єкції, XSS та CSRF, і оцінити реакцію систем моніторингу та сканування. Проведений аналіз

показав, що Burp Suite Pro, AppScan та Splunk забезпечують найвищу точність виявлення загроз, тоді як open-source інструменти (ZAP Proxy, Wazuh) демонструють достатній рівень надійності при мінімальних витратах ресурсів. Результати підтвердили доцільність багаторівневого підходу, який поєднує виявлення вразливостей, централізований моніторинг і автоматизоване реагування на інциденти.

У результаті отриманих даних необхідним є впровадження комбінованих стратегій безпеки, що поєднують технічні, організаційні та аналітичні підходи до захисту корпоративних додатків. Є доцільною інтеграція інструментів сканування вразливостей із SIEM-системами в межах концепцій Zero Trust та DevSecOps, оскільки це забезпечує безперервний моніторинг стану безпеки, своєчасне виявлення загроз і контроль на всіх етапах життєвого циклу додатків.

Особлива увага має приділятися збалансуванню рівня захисту та продуктивності систем, адже результати експериментальної частини довели, що за правильного налаштування сучасні засоби безпеки не створюють критичного навантаження на інфраструктуру та можуть бути ефективно інтегровані без зниження продуктивності.

Отримані результати мають практичне значення для підвищення стійкості корпоративних інформаційно-комунікаційних систем до сучасних кіберзагроз, а також для оптимізації витрат на впровадження комплексних механізмів захисту.

Подальші дослідження доцільно спрямувати на:

– розширення тестового середовища з урахуванням хмарних і контейнеризованих інфраструктур;

– розробку автоматизованих сценаріїв перевірки безпеки на основі алгоритмів машинного навчання;

– удосконалення моделей оцінювання ризиків із використанням динамічних метрик;

– вивчення ефективності інтеграції концепції Zero Trust із системами штучного інтелекту для забезпечення адаптивного реагування на загрози.

Таким чином, отримані результати обґрунтовують необхідність подальшого розвитку інтегрованих рішень із кіберзахисту корпоративних додатків, спрямованих на підвищення їхньої надійності та стійкості до нових типів атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Acunetix. (2025, 05 жовтня). Web Vulnerability Scanner. https://www.acunetix.com/
2. Cisco. (2025, 05 жовтня). Системи виявлення вторгнень. Режим доступу: https://www.cisco.com/c/en/us/products/security/ids-ips/
3. IBM Security. (2025, 05 жовтня). IBM AppScan: Application Security Testing. https://www.ibm.com/security/application-security
4. MITRE Corporation. (2025, 05 жовтня). MITRE ATT&CK Framework. https://attack.mitre.org/
5. NVD. (2025, 05 жовтня). National Institute of Standards and Technology (NIST). Режим доступу: https://nvd.nist.gov
6. OWASP Foundation. (2025, 05 жовтня). OWASP Dependency-Check. https://owasp.org/www-project-dependency-check
7. OWASP. (2025, 05 жовтня). OWASP Top Ten Security Risks. https://owasp.org/www-project-top-ten/
8. SANS Institute. (2025, 05 жовтня). DevSecOps: Інтеграція безпеки в розробку. https://www.sans.org/cyber-security-courses/devsecops/
9. SolarWinds. (2025, 05 жовтня). Security Event Manager (SEM). https://www.solarwinds.com/security-event-manager
10. Splunk. (2025, 05 жовтня). SIEM та XDR для захисту додатків. https://www.splunk.com/en_us/products/enterprise-security.html
11. Wazuh Inc. (2025, 05 жовтня). Security Information and Event Management (SIEM). https://wazuh.com

12. Zero Trust Architecture. (2025, 05 жовтня). Національний інститут стандартів і технологій США. https://www.nist.gov/publications/zero-trust-architecture
13. Kostiuk, Y., Skladannyi, P., Rzaeva , S., Mazur , N., Cherevyk, V., & Anosov, A. (2025). FEATURES OF NETWORK ATTACK IMPLEMENTATION THROUGH TCP/IP PROTOCOLS. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915
14. Tsekhmeister, R., Platonenko, A., Vorokhob , M., Cherevyk, V., & Semeniaka, S. (2025). RESEARCH OF INFORMATION SECURITY PROVISION METHODS IN A VIRTUAL ENVIRONMENT. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *3*(27), 63–71. https://doi.org/10.28925/2663-4023.2025.27.703
15. Vorokhob, M., Kyrychok, R., Yaskevych, V., Dobryshyn, Y., & Sydorenko, S. (2023). MODERN PERSPECTIVES OF APPLYING THE CONCEPT OF ZERO TRUST IN BUILDING A CORPORATE INFORMATION SECURITY POLICY. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233Kriuchkova, L., Skladannyi, P., & Vorokhob, M. (2023). Pre-project solutions for building an authorization system based on the zero trust concept. Cybersecurity: Education, Science, Technique, 3(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242
16. Skuratovskyi, Y., Anosov, A., Kozachok, V., & Brzhevska, Z. (2025). DEVELOPMENT OF A TEST ENVIRONMENT FOR EVALUATING THE EFFECTIVENESS OF IMPLEMENTED APPLICATION-LEVEL SECURITY MEASURES. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *2*(30), 89–98. https://doi.org/10.28925/2663-4023.2025.30.954

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Yevhenii Skuratovskyi
student of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0000-0432-9784
yoskuratovskyi.fitm24m@kubg.edu.ua

Andriy Anosov
PhD, Associate Professor,
Associate Professof the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-2973-6033
a.anosov@kubg.edu.ua

Vitalii Strelnikov
PhD, Associate Professof the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0003-3439-3220
v.strelnikov@kubg.edu.ua

Mykola Kucheriavyi
PhD student
Institute for Problems of Mathematical Machines and Systems
National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0009-0005-0017-9797
bu9free@gmail.com

EXPERIMENTS AND PRACTICAL SOLUTIONS FOR BUILDING A TEST ENVIRONMENT TO ASSESS APPLICATION-LEVEL SECURITY

Abstract. The article examines experimental approaches and practical solutions for building a test environment to assess application-level security. The aim of the research is to create an isolated laboratory infrastructure that simulates a corporate network structure with a DMZ zone, an internal segment, and an attack environment to objectively evaluate the effectiveness of modern security tools. The test environment was implemented using VMware Workstation Pro virtualization and integrated tools such as Burp Suite Pro, AppScan, ZAP Proxy, Acunetix, Splunk, Wazuh, and LogRhythm. A series of experiments were conducted, including simulations of typical application-layer attacks (SQL injection, XSS, CSRF, brute force, and network scanning), along with event log collection and analysis. The experimental results demonstrated that Burp Suite Pro and Splunk provide the highest overall efficiency, while Wazuh and ZAP Proxy offer acceptable quality with minimal resource consumption. It was found that combining scanning, monitoring, and response tools within a multi-layer security model significantly increases system resilience against attacks. Based on the obtained data, practical recommendations were developed for implementing combined application-level protection strategies based on Zero Trust Architecture and DevSecOps principles. The proposed model maintains an optimal balance between security and performance and can be used for building effective monitoring systems, vulnerability testing, and cybersecurity training. The developed environment can also be adapted for testing new protection tools and modeling complex attack scenarios. Future research will focus on improving automated analysis of testing results and expanding the environment's functionality.

Keywords: test environment; application security; Burp Suite; Splunk; Wazuh; DevSecOps; Zero Trust; cyber threats.

REFERENCES

1. Acunetix. (2025, 05 жовтня). Web Vulnerability Scanner. https://www.acunetix.com/
2. Cisco. (2025, 05 жовтня). Системи виявлення вторгнень. Режим доступу: https://www.cisco.com/c/en/us/products/security/ids-ips/
3. IBM Security. (2025, 05 жовтня). IBM AppScan: Application Security Testing. https://www.ibm.com/security/application-security
4. MITRE Corporation. (2025, 05 жовтня). MITRE ATT&CK Framework. https://attack.mitre.org/
5. NVD. (2025, 05 жовтня). National Institute of Standards and Technology (NIST). Режим доступу: https://nvd.nist.gov
6. OWASP Foundation. (2025, 05 жовтня). OWASP Dependency-Check. https://owasp.org/www-project-dependency-check
7. OWASP. (2025, 05 жовтня). OWASP Top Ten Security Risks. https://owasp.org/www-project-top-ten/
8. SANS Institute. (2025, 05 жовтня). DevSecOps: Інтеграція безпеки в розробку. https://www.sans.org/cyber-security-courses/devsecops/
9. SolarWinds. (2025, 05 жовтня). Security Event Manager (SEM). https://www.solarwinds.com/security-event-manager
10. Splunk. (2025, 05 жовтня). SIEM та XDR для захисту додатків. https://www.splunk.com/en_us/products/enterprise-security.html
11. Wazuh Inc. (2025, 05 жовтня). Security Information and Event Management (SIEM). https://wazuh.com
12. Zero Trust Architecture. (2025, 05 жовтня). Національний інститут стандартів і технологій США. https://www.nist.gov/publications/zero-trust-architecture
13. Kostiuk, Y., Skladannyi, P., Rzaeva , S., Mazur , N., Cherevyk, V., & Anosov, A. (2025). FEATURES OF NETWORK ATTACK IMPLEMENTATION THROUGH TCP/IP PROTOCOLS. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915
14. Tsekhmeister, R., Platonenko, A., Vorokhob , M., Cherevyk, V., & Semeniaka, S. (2025). RESEARCH OF INFORMATION SECURITY PROVISION METHODS IN A VIRTUAL ENVIRONMENT. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *3*(27), 63–71. https://doi.org/10.28925/2663-4023.2025.27.703
15. Vorokhob, M., Kyrychok, R., Yaskevych, V., Dobryshyn, Y., & Sydorenko, S. (2023). MODERN PERSPECTIVES OF APPLYING THE CONCEPT OF ZERO TRUST IN BUILDING A CORPORATE INFORMATION SECURITY POLICY. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233Kriuchkova, L., Skladannyi, P., & Vorokhob, M. (2023). Pre-project solutions for building an authorization system based on the zero trust concept. Cybersecurity: Education, Science, Technique, 3(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242
16. Skuratovskyi, Y., Anosov, A., Kozachok, V., & Brzhevska, Z. (2025). DEVELOPMENT OF A TEST ENVIRONMENT FOR EVALUATING THE EFFECTIVENESS OF IMPLEMENTED APPLICATION-LEVEL SECURITY MEASURES. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *2*(30), 89–98. https://doi.org/10.28925/2663-4023.2025.30.954