ТЗ. №5(37)'2025

УДК 004.056.5:004.021

КОМПАРАТИВНИЙ АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ МОДЕЛЮВАННЯ ПЕНТЕСТИНГУ

В.С. Кравчук[1], Я.Ю. Дорогий[1, 2, 3]
[1] *Department of Applied Mathematics and Informatics, Donetsk National Technical University, Drohobych, Ukraine*
[2] *Department of Information Systems and Technologies, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine*
[3] *Department of Intelligent Software Systems, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine*

E-mail: naukovipracidntu@gmail.com

АНОТАЦІЯ

У статті здійснено детальний компаративний аналіз сучасних методів та технологій моделювання пентестингу (тестування на проникнення), що є фундаментальним аспектом забезпечення кібербезпеки в цифровому світі. Автори простежують еволюцію цих підходів: від класичних ручних технік, які потребують високої кваліфікації фахівців, до інноваційних автоматизованих систем, що інтегрують штучний інтелект (ШІ) та машинне навчання (МН). Зокрема, порівнюються різні моделі симуляції вразливостей, а саме популярний Metasploit Framework для емуляції експлойтів, віртуалізовані середовища на базі VirtualBox, VMware чи контейнеризації Docker, які дають змогу створювати ізольовані тестові мережі для імітації реальних атак. Окрему увагу приділено гібридним технологіям, що поєднують традиційні інструменти з AI-алгоритмами для прогнозування й автоматизації атак, наприклад, за допомогою бібліотек TensorFlow, PyTorch або пакетів Scapy для генерації мережевого трафіку. Аналіз проводиться за ключовими критеріями ефективності: точність виявлення вразливостей (з урахуванням хибнопозитивних та хибнонегативних результатів), швидкість виконання тестів, масштабованість для великих систем, витрати обчислювальних ресурсів, рівень помилок і простота інтеграції. Обговорюються переваги кожного методу – наприклад, ручні методи забезпечують глибоке розуміння контексту, тоді як AI-підходи дають змогу обробляти великі обсяги даних у реальному часі – та їхні недоліки, як-от вразливість до загроз, що еволюціонують, чи потреба в постійному навчанні моделей. Особливий акцент робиться на адаптації цих технологій до сучасних сценаріїв, включно із хмарними платформами (AWS, Microsoft Azure, Google Cloud), інтернетом речей (IoT-пристрої з обмеженими ресурсами) та мобільними додатками. Дослідження ґрунтується на емпіричних даних із тестувань на стандартизованих моделях, зокрема OWASP Top 10 для вебвразливостей та NIST Cybersecurity Framework, де показано, що гібридні методи підвищують загальну ефективність на 30–50 % порівняно з традиційними, зменшуючи час на виявлення вразливостей і мінімізуючи ризики. Автори пропонують практичні рекомендації щодо вибору оптимальних технологій для різних типів організацій – від малого бізнесу до великих корпорацій – з урахуванням етичних аспектів (наприклад, дотримання принципів етичного хакінгу), регуляторних вимог (GDPR для захисту даних, ISO 27001 для управління інформаційною безпекою) і потенційних ризиків, як-от несанкціоноване використання інструментів. Стаття є цінним ресурсом для фахівців з кібербезпеки, розробників програмного забезпечення, менеджерів IT-проєктів і дослідників, сприяючи розробці більш стійких стратегій захисту від кіберзагроз у динамічному середовищі цифрових технологій.

Ключові слова: *пентестинг, моделювання вразливостей, компаративний аналіз, штучний інтелект, кібербезпека, Metasploit Framework, OWASP, машинне навчання, віртуалізація, етичний хакинг, TensorFlow, Scapy, хмарні системи, IoT-пристрої.*

Вступ

Зростання кількості кібератак, як-от фішинг, ransomware та витоки даних, свідчить про вразливість сучасних систем, роблячи питання кібербезпеки критичним для бізнесу, державного управління та повсякденного спілкування. За даними звіту Verizon Data Breach Investigations Report 2025, у регіоні APAC System Intrusion становить 83 % порушень, а Ransomware – 51 % [1]. Крім того, глобальні збитки від кіберзлочинності очікуються на рівні $10,5 трлн щорічно до 2025 року, з потенційним зростанням до $12,2 трлн до 2031 року [2]. У цьому контексті

ISSN 2786-9024

пентестинг (penetration testing), або тестування на проникнення, стає невід’ємним інструментом для виявлення й усунення потенційних загроз до їхньої реалізації зловмисниками. Пентестинг імітує дії хакерів, даючи змогу організаціям оцінити рівень захисту своїх систем і розробити ефективні стратегії оборони.

Однак традиційні методи пентестингу, які базуються на ручному аналізі та стандартних інструментах, часто стикаються з обмеженнями: вони потребують значних часових і людських ресурсів, не завжди масштабовані для великих мереж і не здатні оперативно реагувати на нові типи атак, що еволюціонують завдяки ШІ та МН. Згідно з CompTIA’s State of Cybersecurity 2025 Report, навички ШІ є головним викликом для прискорення впровадження ШІ в кібербезпеці: 70 % компаній перебувають на ранніх етапах освіти чи тестування [3]. З появою хмарних технологій, IoT та розподілених систем, як-от AWS чи Azure, моделювання пентестингу потребує інноваційних підходів. Саме тому компаративний аналіз методів та технологій моделювання пентестингу є актуальним завданням, що дає змогу систематизувати знання та визначити оптимальні рішення для різних сценаріїв, враховуючи тренди, зокрема AI-powered атаки, які стали головною турботою для 80 % CISO [4].

Цю статтю присвячено порівняльному огляду сучасних методів моделювання пентестингу, від класичних симуляцій вразливостей до гібридних систем на базі ШІ. Розглянемо еволюцію цих технологій, починаючи з інструментів на кшталт Metasploit Framework, які дають змогу емулювати експлойти в контрольованому середовищі, до віртуалізованих платформ (VirtualBox, Docker), що створюють ізольовані тестові мережі. Особливу увагу буде приділено інтеграції МН, наприклад, через бібліотеки TensorFlow чи Scapy, для автоматизованого прогнозування атак і генерації сценаріїв. Аналіз базуватиметься на критеріях ефективності: точність, швидкість, масштабованість, витрати ресурсів та рівень помилок.

Метою дослідження є не лише порівняння переваг і недоліків кожного методу, але й надання практичних рекомендацій для впровадження в реальних умовах, з урахуванням етичних норм (етичний хакинг) і регуляторних стандартів (GDPR, ISO 27001). Для обґрунтування висновків використано емпіричні дані з тестувань на моделях OWASP та NIST, які демонструють, як гібридні підходи можуть підвищити ефективність на 30–50 %.

Постановка проблеми дослідження

Проблема дослідження полягає у відсутності систематичного компаративного аналізу методів та технологій моделювання пентестингу, що ускладнює вибір оптимальних підходів для різних сценаріїв – від традиційних симуляцій до гібридних AI-систем. Існуючі дослідження фокусуються на окремих техніках, але ігнорують критерії ефективності (точність, швидкість, масштабованість, витрати, помилки) та адаптацію до загроз, що еволюціонують, як-от AI-генеровані атаки чи вразливості в IoT.

З огляду на вищенаведене метою цього дослідження є надання детального компаративного аналізу методів і технологій моделювання пентестингу, застосовних у кібербезпеці, з акцентом на їхню ефективність, сфери використання (від хмарних систем до IoT-пристроїв) та потенціал інтеграції з штучним інтелектом і машинним навчанням.

Для досягнення цієї мети систематизовано традиційні (ручні та симуляційні) та сучасні (гібридні та AI-орієнтовані) підходи, проаналізовано їхні особливості (наприклад, точність виявлення вразливостей, швидкість і масштабованість), проведено порівняльну оцінку на основі емпіричних даних із моделей OWASP та NIST, а також визначено ключові виклики (етичні ризики, регуляторні обмеження) і перспективи розвитку (автоматизація та адаптація до загроз, що еволюціонують).

Матеріали та методи дослідження

Дослідження зосереджено на порівнянні методів та технологій моделювання пентестингу в кібербезпеці, використовуючи наукові публікації, технічні звіти й огляди з авторитетних джерел, як-от IEEE, Springer, MDPI, arXiv, а також матеріали організацій, зокрема OWASP, NIST, XM Cyber і Picus Security, до 2025 року. Аналіз охопив літературу про симуляційне моделювання (наприклад, Metasploit Framework), віртуалізацію (VirtualBox, Docker), агентно-орієнтоване моделювання, машинне навчання (TensorFlow, Scapy), графові моделі та великі мовні моделі. Кейси застосування, зокрема моделі OWASP Top 10, фреймворк NIST Cybersecurity, платформи BAS (SCYTHE, AttackIQ) і графові інструменти (Neo4j, Maltego), стали основою для оцінки практичної реалізації методів.

Для аналізу застосовано фундаментальні та прикладні методи. Аналіз і синтез допомогли систематизувати характеристики методів, порівняльний аналіз зіставив традиційні (ручні та симуляційні) та новітні (гібридні та AI-орієнтовані) підходи за ефективністю, масштабованістю й адаптивністю, а системний підхід розглядав методи як взаємопов’язані елементи кібербезпеки. Огляд літератури та класифікація методів дали змогу зібрати дані про принципи роботи та приклади застосування, тоді як порівняльна оцінка, зокрема BAS проти традиційного тестування на проникнення, виявила їхні сильні та слабкі сторони. Аналіз кейсів (наприклад, використання CrowdStrike для машинного навчання в моделюванні атак чи GALLIUM APT для агентного моделювання) доповнив

Copyright © 2025, ОТА.

дослідження емпіричними даними з тестувань на моделях OWASP та NIST.

Методологічно дослідження базувалося на об'єктивності й науковій достовірності, використовуючи програмні інструменти для систематизації літератури (Mendeley, Zotero) та обробки текстів. Поєднання фундаментальних методів, зокрема абстрагування для виділення ключових аспектів, із прикладними, як-от аналіз кейсів, забезпечило цілісне розуміння методів моделювання. Особлива увага приділялася синергії підходів, включно з інтеграцією AI для прогнозування вразливостей та автоматизації тестів, що є основою для створення адаптивних систем кіберзахисту.

Аналіз методів і технологій моделювання

У контексті пентестингу моделювання відіграє ключову роль у симуляції атак, виявленні вразливостей та оцінці ефективності захисних механізмів без ризику для реальних систем. Аналіз методів і технологій моделювання дає змогу систематизувати традиційні та сучасні підходи, оцінити їх за критеріями ефективності (точність виявлення, швидкість, масштабованість, витрати ресурсів, рівень помилок), а також визначити перспективи інтеграції з новими технологіями, зокрема ШІ та МН. Цей розділ базується на огляді літератури й емпіричних даних, охоплюючи симуляційні, віртуалізовані, агентно-орієнтовані та гібридні методи, з акцентом на їх застосування в хмарних середовищах (AWS, Azure), IoT-пристроях і розподілених мережах.

Традиційні методи моделювання пентестингу зосереджені на ручному або напівавтоматизованому імітації атак, використовуючи інструменти для симуляції вразливостей у контрольованому середовищі. Одним із ключових є симуляційне моделювання на базі фреймворків, а саме Metasploit Framework, який дає змогу емулювати експлойти, сканування мереж та етапи атаки за моделлю Cyber Kill Chain (від розвідки до ексфільтрації даних). Metasploit інтегрує модулі для моделювання вразливостей з бази CVE, забезпечуючи точність на рівні 80–90 % для відомих загроз, але потребує значних ресурсів для налаштування [5–6].

Віртуалізовані середовища, наприклад VirtualBox або Docker, створюють ізольовані тестові мережі для моделювання реальних сценаріїв. Docker контейнери дають змогу швидко розгортати віртуальні машини з вразливими сервісами, забезпечуючи масштабованість для мереж до 100 вузлів, але обмежені в динамічних змінах (наприклад, адаптація до MTD – Moving Target Defense) [7]. Ці методи ефективні для статичних сценаріїв, з швидкістю виконання 1–5 годин на тест, але мають високий рівень помилок (до 20 % хибнопозитивних) через відсутність автоматизації [8].

Переваги традиційних методів у глибокому розумінні контексту та адаптації до конкретних систем, але недоліки – це низька масштабованість і залежність від експертів, що робить їх менш придатними для великих мереж або швидких загроз.

Сучасні підходи інтегрують ШІ та МН для автоматизації моделювання, підвищуючи ефективність на 30–50 %. Агентно-орієнтоване моделювання (ABM) представляє атакерів та захисників як автономні агенти, симулюючи взаємодії в динамічних середовищах. Наприклад, фреймворки на базі reinforcement learning (RL), як-от DQN або POMDP (Partially Observable Markov Decision Processes), моделюють атаки як стохастичні процеси, де стан мережі описується графом G = (V, E, X) з вузлами (пристрої), ребрами (з'єднання) та атрибутами (вразливості, CVSS-бали) [9].

Інструменти на кшталт TensorFlow або Scapy генерують мережевий трафік для прогнозування атак, надаючи можливість симулювати до 1000 вузлів з динамічними змінами (p_change до 0.5), зменшуючи час тестування до хвилин [10].

Гібридні технології, зокрема Breach and Attack Simulation (BAS) платформи (SCYTHE, AttackIQ), поєднують симуляцію з реальними даними, тестуючи весь cyber kill chain. BAS автоматизує атаки на багатошарових захистах (NGFW, EDR, WAF), забезпечуючи безперервне тестування з низьким ризиком, на відміну від ручних пентестів [11].

Графові моделі (Neo4j, Maltego) візуалізують шляхи атак, інтегруючи MITRE ATT&CK для моделювання тактик, з точністю виявлення 95 % для відомих векторів [12]. Великі мовні моделі (LLM) додають інтелекту, генеруючи сценарії атак для IoT, з фокусом на етичні аспекти.

Компаративний аналіз. Компаративний аналіз методів і технологій моделювання пентестингу проводиться з метою об'єктивного порівняння традиційних, сучасних та гібридних підходів. Для оцінки введено критерії порівняння із числовою шкалою від 1 до 10, де 1 означає найнижчий рівень (наприклад, низька точність, висока витрата ресурсів), а 10 – найвищий (висока точність, низька витрата). Критерії базуються на емпіричних даних з літератури та передбачають:

– *точність виявлення вразливостей* – оцінює, наскільки метод правильно ідентифікує реальні загрози без хибнопозитивних / хибнонегативних результатів (вища оцінка – вища точність);

– *швидкість виконання* – вимірює час на тестування;

– *масштабованість* – можливість застосування до великих мереж (вища оцінка – краща адаптація до 1000+ вузлів);

– *витрати ресурсів* – обчислювальні, людські та фінансові витрати (вища оцінка – нижчі витрати);

– рівень помилок – частота помилок (вища оцінка – нижчий рівень помилок).

Оцінки присвоєно на основі аналізу джерел, як-от порівняльні дослідження методологій пентестингу [13] та оглядів інструментів для моделювання [5]. Методи згруповано за типами: традиційні (наприклад, Metasploit Framework, VirtualBox), сучасні (агентно-орієнтовані з RL, Scapy), гібридні (BAS-платформи як SCYTHE, AttackIQ з інтеграцією AI) (див. таблицю 1).

Традиційні методи, а саме Metasploit Framework для симуляції експлойтів та VirtualBox для віртуалізованих мереж, демонструють високу точність (8/10) завдяки ручному контролю та фокусу на відомих вразливостях з бази CVE, що зменшує хибнопозитивні результати [14]. Однак їхня швидкість низька (4/10), оскільки тести потребують часу на налаштування та виконання, особливо для статичних сценаріїв. Масштабованість обмежена (5/10) до середніх мереж (до 100 вузлів) через залежність від ручної конфігурації, а витрати ресурсів середні (6/10) з потребою у кваліфікованих фахівцях. Рівень помилок прийнятний (7/10), але зростає в динамічних середовищах, як-от хмарні системи AWS чи Azure, де відсутня автоматизація призводить до пропуску загроз, що еволюціонують.

Сучасні методи, включно з агентно-орієнтованим моделюванням з reinforcement learning (RL) та інструментами на кшталт Scapy для генерації трафіку, виділяються високою швидкістю (8/10), надаючи реальний час обробки (хвилини) завдяки автоматизації прогнозування атак. Масштабованість висока (9/10), оскільки RL-моделі (наприклад, DQN) адаптуються до великих мереж (1000+ вузлів) з динамічними змінами, як у IoT-пристроях. Точність дещо нижча (7/10) через можливі упередження в навчанні моделей, а витрати ресурсів вищі (5/10) через потребу в GPU для TensorFlow чи PyTorch. Рівень помилок середній (6/10), із ризиком хибнонегативних у невідомих сценаріях, але це компенсується адаптивністю до AI-powered атак.

Гібридні методи, а саме Breach and Attack Simulation (BAS) з інтеграцією AI (наприклад, AttackIQ з TensorFlow), досягають найвищої точності (9/10) завдяки комбінації симуляції та реальних даних, зменшуючи помилки до 5–10 %. Швидкість висока (9/10) з автоматизацією всього cyber kill chain, масштабованість добра (8/10) для розподілених систем, витрати ресурсів оптимальні (7/10) з балансом між автоматизацією та людським наглядом. Рівень помилок низький (8/10), особливо в хмарних та IoT-сценаріях, де гібридні підходи підвищують ефективність на 30–50 % порівняно з традиційними, як показано в тестах OWASP та NIST [15].

Загалом гібридні методи перевершують інші в більшості критеріїв, роблячи їх оптимальними для сучасних організацій, тоді як традиційні підходять для невеликих, статичних систем. Аналіз підкреслює необхідність інтеграції AI для адаптації до загроз, що еволюціонують, з рекомендаціями щодо вибору залежно від розміру організації та типу інфраструктури.

Обговорення та перспективи розвитку дослідження

У розділі аналізу методів і технологій моделювання пентестингу було продемонстровано, що гібридні підходи, які поєднують традиційні симуляції (наприклад, Metasploit Framework) з елементами ШІ та МН, перевершують класичні методи за критеріями ефективності, швидкості та масштабовальності. Емпіричні дані з тестувань на моделях OWASP та NIST підтверджують підвищення ефективності на 30–50 %, особливо в хмарних середовищах (AWS, Azure) та системах IoT, де динамічні загрози потребують адаптивності. Однак традиційні методи зберігають перевагу в глибокому контекстному розумінні, тоді як сучасні AI-орієнтовані інструменти (наприклад, TensorFlow чи Scapy) схильні до упереджень у моделях і потребують постійного навчання, що може призводити до хибнопозитивних результатів у 10–20 % випадків [16]. Обмеження дослідження стосуються фокуса на теоретичних моделях без широкого емпіричного тестування в реальних організаціях, а також ігнорування факторів, як-от вартість впровадження, яка для гібридних систем може сягати 20–30 % від бюджету на кібербезпеку. Це підкреслює необхідність

Табл. 1. Компаративний аналіз методів

Метод / критерій	Точність	Швидкість	Масштабованість	Витрати ресурсів	Рівень помилок
Традиційні (Metasploit, VirtualBox)	8	4	5	6	7
Сучасні (RL-агенти, Scapy)	7	8	9	5	6
Гібридні (BAS з AI, TensorFlow)	9	9	9	7	8

Copyright © 2025, ОТА.

балансу між автоматизацією та людським наглядом, щоб уникнути етичних ризиків, як-от несанкціоноване використання інструментів, відповідно до стандартів GDPR та ISO 27001.

Перспективи розвитку дослідження пов'язані з інтеграцією передових технологій, що формують майбутнє кібербезпеки. Згідно з прогнозами на 2025 рік, ключовим трендом стане використання генеративного ШІ (genAI) для автоматизованого створення сценаріїв атак, що дасть змогу моделювати складні загрози, зокрема AI-powered фішинг чи інсайдерські атаки, з ростом ефективності на 30 % [17]. Гібридний пентестинг, що поєднує людських експертів з AI-інструментами (наприклад, PentestGPT чи DeepExploit), набуде поширення, особливо в безперервному тестуванні, інтегрованому з CI/CD-пайплайнами, для оперативного реагування на загрози, що еволюціонують. У контексті IoT та хмарних систем перспективним є розвиток агентно-орієнтованого моделювання з елементами теорії ігор, де атаки моделюються як стохастичні процеси, з використанням LLM для генерації динамічних векторів. Крім того, загрози від shadow AI – несанкціонованих моделей в організаціях – потребуватимуть нових методів моделювання для оцінки ризиків з акцентом на етичні аспекти й регуляторні вимоги.

Майбутні дослідження повинні фокусуватися на інтеграції квантових обчислень для моделювання постквантових атак, а також на розробці стандартів для AI в пентестингу, щоб зменшити залежність від людських ресурсів і підвищити доступність для малого бізнесу. Очікується зростання ролі автоматизованих платформ BAS (наприклад, SCYTHE чи AttackIQ) з елементами ML, що скоротить час тестування до реального часу та зменшить втому від сповіщень (alert fatigue). Загалом перспективи розвитку спрямовані на створення адаптивних, стійких систем кіберзахисту, що інтегрують ШІ для проактивного виявлення загроз, з потенціалом зростання ринку пентестингу на 15–20 % щорічно до 2030 року [18]. Це дослідження може слугувати основою для подальших емпіричних робіт, спрямованих на практичне впровадження гібридних моделей у різних галузях.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов'язаних даних.

ЛІТЕРАТУРА

[1] Verizon, "2025 Data Breach Investigations Report," Verizon, 2025. [Онлайн]. URL: https://surl.li/qsfajk. Дата звернення: 25.09.2025.

[2] Cybersecurity Ventures, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Apr. 2025. [Онлайн]. URL: https://surl.li/ujmskz. Дата звернення: 25.09.2025.

[3] CompTIA, "State of Cybersecurity 2025," 2025. [Онлайн]. URL: https://surl.lu/mjjnfk. Дата звернення: 25.09.2025.

[4] A. Angner et al., "AI Creates New Cyber Risks. It Can Help Resolve Them, Too," Boston Consulting Group, Jul. 2025. [Онлайн]. URL: https://surl.li/jybvzv. Дата звернення: 25.09.2025.

[5] M. Khalil, "Penetration Testing Methodology 2025: Complete Guide," DeepStrike, Aug. 2025. [Онлайн]. URL: https://surl.li/lossfh. Дата звернення: 25.09.2025.

[6] V. Kravchuk, N. Maslova, and I. Dorohyi, "AUTOMATED XSS VULNERABILITY DETECTION IN WEB APPLICATIONS BASED ON A MULTI-AGENT APPROACH", SP DonNTU. OTA, vol. 3, no. 4 (36), pp. 13–26, May 2025.

[7] "Simulating Penetration Testing Using a Modeling Framework," Assurant Cyber, Aug. 2023. [Онлайн]. URL: https://surl.li/hqgzow. Дата звернення: 25.09.2025.

[8] "Vulnerability Assessment vs Penetration Testing 2025," DeepStrike, May 2025. [Онлайн]. URL: https://surl.li/fjiytg. Дата звернення: 25.09.2025.

[9] X. Wang et al., "A Unified Modeling Framework for Automated Penetration Testing," arXiv, Feb. 2025. [Онлайн]. URL: https://surl.li/fixacj. Дата звернення: 25.09.2025.

[10] "Simulation in Cybersecurity: Understanding Techniques, Applications, and Goals," ResearchGate, Aug. 2025. [Онлайн]. URL: https://surl.li/pddbjh. Дата звернення: 25.09.2025.

[11] "Breach and Attack Simulation vs. Penetration Testing," Picus Security, May 2025. [Онлайн]. URL: https://surl.li/lflczz. Дата звернення: 25.09.2025.

[12] "Comparative analysis of penetration testing approaches for IoT devices," ResearchGate, Jun. 2024. [Онлайн]. URL: https://surl.li/hnpome. Дата звернення: 25.09.2025.

[13] A Comparative Study of Penetration Testing Methodologies and Tool Utilization in Cybersecurity, ResearchGate, Aug. 2025. [Онлайн]. URL: https://surl.li/zyinek. Дата звернення: 25.09.2025.

[14] Penetration Testing in 2025: Methods, Technologies & Practices, CyCognito. [Онлайн]. URL: https://surl.li/jqugpc. Дата звернення: 25.09.2025.

[15] Penetration Testing ROI: Executive Guide 2025, Redbot Security. [Онлайн]. URL: https://surl.li/ugqzas. Дата звернення: 25.09.2025.

[16] "A Comparative Study of Penetration Testing Methodologies and Tool Utilization in Cybersecurity," ResearchGate, Aug. 2025. [Онлайн]. URL: https://surl.li/oammic. Дата звернення: 25.09.2025.

[17] "Pentesting Statistics 2025: Key Insights and Emerging Trends," ZeroThreat, Jul. 2025. [Онлайн]. URL: https://surl.lt/tlejih. Дата звернення: 25.09.2025.
[18] "10 Cyber Security Trends For 2025," SentinelOne, Aug. 2025. [Онлайн]. URL: https://surl.li/yclkhx. Дата звернення: 25.09.2025.

COMPARATIVE ANALYSIS OF METHODS AND TECHNOLOGIES FOR PENETRATION TESTING MODELING

Vitaly Kravchuk, Iaroslav Dorohyi

The article conducts a detailed comparative analysis of contemporary methods and technologies for modeling penetration testing (pentesting), a fundamental aspect of ensuring cybersecurity in the digital world. The authors trace the evolution of these approaches: from classical manual techniques that require high expertise from specialists to innovative automated systems integrating artificial intelligence (AI) and machine learning (ML). Specifically, various vulnerability simulation models are compared, such as the popular Metasploit Framework for exploit emulation, virtualized environments based on VirtualBox, VMware, or containerization with Docker, which enable the creation of isolated test networks for simulating real attacks. Special attention is given to hybrid technologies that combine traditional tools with AI algorithms for attack prediction and automation, for example, using libraries like TensorFlow, PyTorch, or Scapy packages for generating network traffic. The analysis is performed based on key efficiency criteria: accuracy in vulnerability detection (considering false positives and false negatives), test execution speed, scalability for large systems, computational resource costs, error rates, and ease of integration. The advantages of each method are discussed–for instance, manual methods provide deep contextual understanding, while AI approaches enable real-time processing of large data volumes–and their disadvantages, such as vulnerability to evolving threats or the need for continuous model training. Particular emphasis is placed on adapting these technologies to modern scenarios, including cloud platforms (AWS, Microsoft Azure, Google Cloud), Internet of Things (IoT devices with limited resources), and mobile applications. The research is grounded in empirical data from tests on standardized models, such as OWASP Top 10 for web vulnerabilities and NIST Cybersecurity Framework, where it is shown that hybrid methods increase overall efficiency by 30-50% compared to traditional ones, reducing vulnerability detection time and minimizing risks. The authors offer practical recommendations for selecting optimal technologies for different types of organizations–from small businesses to large corporations–considering ethical aspects (e.g., adherence to ethical hacking principles), regulatory requirements (GDPR for data protection, ISO 27001 for information security management), and potential risks, such as unauthorized tool usage. The article serves as a valuable resource for cybersecurity professionals, software developers, IT project managers, and researchers, contributing to the development of more resilient strategies for protection against cyber threats in a dynamic digital technology environment.

Keywords: *pentesting, vulnerability modeling, comparative analysis, artificial intelligence, cybersecurity, Metasploit Framework, OWASP, machine learning, virtualization, ethical hacking, TensorFlow, Scapy, cloud systems, IoT devices.*

REFERENCES

[1] Verizon, "2025 Data Breach Investigations Report," Verizon, 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/qsfajk.
[2] Cybersecurity Ventures, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Apr. 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/ujmskz.
[3] CompTIA, "State of Cybersecurity 2025," 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.lu/mjjnfk.
[4] A. Angner et al., "AI Creates New Cyber Risks. It Can Help Resolve Them, Too," Boston Consulting Group, Jul. 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/jybvzv.
[5] M. Khalil, "Penetration Testing Methodology 2025: Complete Guide," DeepStrike, Aug. 2025. [OnlineAccessed: Sep. 25, 2025]. URL: https://surl.li/lossfh.
[6] V. Kravchuk, N. Maslova, and I. Dorohyi, “AUTOMATED XSS VULNERABILITY DETECTION IN WEB APPLICATIONS BASED ON A MULTI-AGENT APPROACH”, SP DonNTU. OTA, vol. 3, no. 4 (36), pp. 13–26, May 2025.
[7] "Simulating Penetration Testing Using a Modeling Framework," Assurant Cyber, Aug. 2023. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/hqgzow.
[8] "Vulnerability Assessment vs Penetration Testing 2025," DeepStrike, May 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/fjiytg.
[9] X. Wang et al., "A Unified Modeling Framework for Automated Penetration Testing," arXiv, Feb. 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/fixacj.
[10] "Simulation in Cybersecurity: Understanding Techniques, Applications, and Goals," ResearchGate, Aug. 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/pddbjh.
[11] "Breach and Attack Simulation vs. Penetration Testing," Picus Security, May 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/lflczz.
[12] "Comparative analysis of penetration testing approaches for IoT devices," ResearchGate, Jun. 2024. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/hnpome.

Copyright © 2025, OTA.

[13] A Comparative Study of Penetration Testing Methodologies and Tool Utilization in Cybersecurity, ResearchGate, Aug. 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/zyinek.

[14] Penetration Testing in 2025: Methods, Technologies & Practices, CyCognito. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/jqugpc.

[15] Penetration Testing ROI: Executive Guide 2025, Redbot Security. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/ugqzas.

[16] "A Comparative Study of Penetration Testing Methodologies and Tool Utilization in Cybersecurity," ResearchGate, Aug. 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/oammic.

[17] "Pentesting Statistics 2025: Key Insights and Emerging Trends," ZeroThreat, Jul. 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.lt/tlejih.

[18] "10 Cyber Security Trends For 2025," SentinelOne, Aug. 2025. [Online]. Accessed: Sep. 25, 2025. URL: https://surl.li/yclkhx.

Стаття надійшла до редакції 30.09.2025
Стаття прийнята 12.10.2025
Статтю опубліковано