УДК 004.056

Ю. Баришев

ПОРІВНЯЛЬНИЙ АНАЛІЗ ОПЕРАЦІЙНИХ СИСТЕМ ДЛЯ ЗАДАЧ ЕТИЧНОГО ХАКІНГУ

Вінницький національний технічний університет

Анотація

Розглянуто задачу використання операційних систем в задачах кібербезпеки, пов'язаних з етичним хакінгом. Визначено недостатність уваги, яка приділяється низці операційних систем, розроблених для виконання цих завдань. Виконано постановку мети дослідження. Наведено результати ідентифікації критеріїв аналізу. На основі цих критеріїв порівняно низку відомих операційних систем. На основі аналізу розроблено практичні рекомендації щодо їх застосування під час розв'язання окремих задач етичного хакінгу.

Ключові слова: кібербезпека, етичний хакінг, операційні системи, тестування на проникнення, аналіз вразливостей, криптографія.

Abstract

The task of an operating systems usage in cyber security tasks related to ethical hacking is considered. The lack of attention paid to a number of operating systems developed to perform these tasks is determined. The research goal is stated. The results of analysis criteria identification are presented. Based on these criteria, a number of known operating systems are compared. Based on the analysis, practical recommendations for their application when individual ethical hacking tasks solving are developed.

Keywords: cyber security, ethical hacking, operating systems, penetration testing, vulnerability analysis, cryptography.

Вступ

Діяльність будь-якого фахівця залежить не лише від його знань та навичок, але й від інструментів, які йому доступні. І фахівці з кібербезпеки, які займаються напрямом етичного хакінгу, не є виключенням. Деякі операційні системи, зокрема, Kali Linux [1] вважаються ледь не промисловим стандартом для задач тестування на проникнення. Деякі інші, наприклад, BlackArch [2] та Parrot Security OS [3] є менш популярними, але все ж відомими і розглядаються як альтернатива до Kali Linux [4, 5]. Популярність цих операційних систем обумовлює орієнтування формальної та неформальної освіти саме на них, оминаючи увагою альтернативні рішення. Водночас крім цих операційних систем відома низка інших, які варті уваги під час вибору інструментів, і які можуть стати кориснішими для виконання робочих завдань, ніж більш популярні аналоги [4, 6]. Таким чином постає актуальна задача порівняльного аналізу операційних систем з метою визначення їх можливостей для розв'язання різних задач етичного хакінгу.

Метою даного дослідження є покращення проведення досліджень з виявлення вразливостей інформаційних систем шляхом порівняльного аналізу наборів інструментів, які для цього використовуються.

Для досягнення мети необхідно виконати такі завдання:

- визначити критерії аналізу;
- виконати порівняльний аналіз операційних систем;
- висунути практичні рекомендації щодо використання операційних систем.

Визначення критеріїв аналізу

Задача визначення критеріїв аналізу інструментів до етичного хакінгу наразі ускладнена відсутністю уніфікованого тлумачення цього фаху. Так в Україні набір навичок етичного хакера згадується в низці професійних стандартів, з-поміж яких в першу чергу варто відзначити такі:

- аналітик з оцінки вразливостей [7];
- фахівець з тестування систем захисту інформації [8];
- фахівець з кібердосліджень та розробок систем безпеки [9].

Крім того, в рамці навичок професіоналів з кібербезпеки Європейського Союзу [10] "етичний хакер" згадується як альтернативна назва до фахівців з тестування на проникнення (penetration tester). Окрім документів нормативно-правового регулювання галузі кібербезпеки, під час ідентифікації критеріїв аналізу також необхідно звертати увагу і на бачення підприємств та установ, які формують ринок праці для цих фахівців [11]. В роботі [12] було представлено результати порівняльного аналізу цих професійних стандартів.

Таким чином, на основі аналізу цих джерел [7-12] було визначено такі основні трудові функції, з якими зустрічаються фахівці з етичного хакінгу:

- виявлення відомих вразливостей в інформаційних системах або їх підсистемах;
- дослідження інформаційних систем з метою виявлення загроз нульового дня;
- проведення досліджень окремих програмних продуктів щодо наявності шкідливого або недокументованого коду;
- проведення досліджень проєктів рішень, які плануються до впровадження.

При цьому об’єктами дослідження зазвичай постають [10-12]:

- операційні системи (ОС);
- прикладні застосунки (ПЗ);
- комп’ютерна мережа (КМ);
- підсистеми автентифікації користувачів (АК);
- підсистеми криптографічного захисту (КГ);
- документація;
- бізнес-процеси підприємства.

Оскільки дослідження останніх двох об’єктів наразі немає інструментів для дослідження, а більше залежить від знань та навичок етичних хакерів, то вони не будуть розглядатись в подальшому в межах цього дослідження. Проте вони залишаються важливим об’єктом, аналіз якого є критичним для виявлення вразливостей інформаційних систем.

Результати порівняльного аналізу

Відповідно до визначених критеріїв було проаналізовано низку операційних систем. Результати порівняльного аналізу наведено в таблиці 1 [1-6].

Табл. 1.

Операційні системи для задач етичного хакінгу	База	Кількість інструментів (порядок)	Об’єкт тестування				
			ОС	ПЗ	КМ	АК	КГ
Kali Linux	Debian	600	+/-	+/-	+	+	-
Parrot Security OS	Debian	700	+/-	+/-	+/-	+	-
BlackArch	Arch	2800	+/-	+	+	+	+/-
BlackBox	Ubuntu	400	-	+/-	+	+/-	-
Samurai Web Testing Framework	Ubuntu	200	-	+/-	+/-	+	-
CAINE	Ubuntu	200	+	+	-	+/-	+/-
Pentoo Linux	Gentoo	500	+/-	+/-	+/-	+	+/-
Fedora Security Lab	Fedora	300	+	+	-	+/-	-

Як видно з таблиці 1 напрям дослідження криптографічного захисту має недостатнє покриття інструментами. Це пояснюється тим, що криптоаналіз є наукомісткою галуззю. Більше того, часто особливості організації криптографічних методів стають ключовими для визначення вразливостей. Відповідно під час їх дослідження варто звертати увагу на таке:

- тип методу (шифр, геш-функція, протокол тощо);
- алгебраїчна структура, яка використовується методом;
- конкретні технічні рішення, ухвалені під час реалізації методу;
- керування ключами;
- особливості синхронізації/взаємодії з іншими пристроями, якщо це передбачено методом;
- статистичні показники впливу вхідних даних на вихідні;
- розподіл вихідних значень.

З-поміж перелічених особливостей лише останні дві властивості мають порівняно універсальний характер і дозволяють розробляти автоматизовані засоби тестування. Решта властивостей має передбачати реалізацію низки вузькоспеціалізованих засобів, які будуть актуальними для обмеженого кола методів, або лише для одного криптографічного методу. Тим не менш, розроблення таких засобів для стандартизованих або поширених методів залишається актуальною.

Висновки

Аналіз операційних систем для етичного хакінгу показав їх різноманіття, а також недостатність уваги, яка приділяється деяким менш відомим системам. Зокрема аналіз інструментів Fedora Security Lab показав, що вона завдяки своїй спеціалізації краще підходить для виконання завдань з цифрової криміналістики та дослідження окремих обчислювальних засобів, ніж більш популярні системи, що мають ширшу мету їх застосування.

Ще одним результатом аналізу є виявлення недостатності інструментів для аналізу підсистем криптографічного захисту. Визначено, що причинами такого стану є складність, наукомісткість та комплексність криптографічних методів для розроблення автоматизованих методів аналізу, що залишатимуться актуальними протягом тривалого часового періоду. З метою удосконалення поточного стану в тезах запропоновано вектори розроблення інструментів для покращення ситуації.

Також важливо відзначити, що зміна ландшафту загроз постійно впливає на вимоги щодо функціональності засобів для етичного хакінгу. Відповідно аналітичні відомості, представлені в цьому та подібних дослідженнях швидко втрачають актуальність, а тому потребують періодичного повторення з урахуванням актуалізації вимог.

Подальші дослідження в цьому напрямі доцільно провадити в напрямі аналізі окремих інструментів для окремих об’єктів аналізу, а також розроблення інструментів для аналізу підсистем криптографічного захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. g0tmi1k. What is Kali Linux? 19.09.2024. URL: https://www.kali.org/docs/introduction/what-is-kali-linux/ (last accessed: 11.02.2026).

2. The BlackArch Linux Guide. URL: https://blackarch.org/blackarch-guide-en.pdf (last accessed: 11.02.2026).

3. What is ParrotOS? .URL: https://parrotsec.org/docs/introduction/what-is-parrot/ (last accessed: 11.02.2026).

4. C. Kumar. 11 FREE Operating System for Penetration Testing & Digital Forensics. 22.12.2024. URL: https://geekflare.com/cybersecurity/penetration-testing-os/ (last accessed: 11.02.2026).

5. Fahid. Top 10 Operating Systems Every Ethical Hacker Should Use in 2025. 15.10.2025. URL: https://www.ethicalhackinginstitute.com/blog/Top-10-Operating-Systems-Every-Ethical-Hacker-Should-Use (last accessed: 11.02.2026).

6. Cyber Sapiens. Top 10 Operating Systems for Ethical Hacking and Penetration Testing [Experts Picks] 28.02.2025. URL: https://cybersapiens.com.au/cyber-awareness/top-10-operating-systems-for-ethical-hacking-and-penetration-testing-experts-picks/ (last accessed: 11.02.2026).

7. Професійний стандарт. Аналітик з оцінки вразливостей. Затверджено наказом Адміністрації ДССЗЗІУ 23 січня 2024 року № 38. 26 с. URL: https://register.nqa.gov.ua/uploads/0/565-analitik_z_ocinki_vrazlivostej_v_2.pdf (дата звернення: 11.02.2026).

8. Професійний стандарт. Фахівець з тестування систем захисту інформації. Затверджено наказом Адміністрації ДССЗЗІУ 23 січня 2024 року № 38. 23 с. URL: https://register.nqa.gov.ua/uploads/0/577-fahivec_z_testuvanna_sistem_zahistu_informacii_v_2.pdf (дата звернення: 11.02.2026).

9. Професійний стандарт. Фахівець з кібердосліджень та розробок систем безпеки. Затверджено наказом Адміністрації ДССЗЗІУ 23 січня 2024 року № 38. 29 с. URL: https://register.nqa.gov.ua/uploads/0/573-fahivec_z_kiberdoslidzen_ta_rozrobok_sistem_bezpeki_v_2.pdf (дата звернення: 11.02.2026).

10. ENISA. ECSF: European Cybersecurity Skills Framework. 19.09.2022. 27 p. URL: https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf (last accessed: 11.02.2026).

11. Global Skill Development Council. Ethical Hacker Skills To have in 2025. 25.04.2024. URL: https://www.gsdcouncil.org/blogs/ethical-hacker-skills (last accessed: 11.02.2026).

12. Баришев Ю. В. Аналіз бачення фахівців з етичного хакінгу в професійних стандартах України та ЄС. Матеріали LIV науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2025) : збірник доповідей. Вінниця : ВНТУ, 2025 С. 575-577. URL: https://press.vntu.edu.ua/index.php/vntu/catalog/view/904/1576/2888-1 (дата звернення: 11.02.2026).

Баришев Юрій Володимирович — канд. техн. наук, доцент кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e- mail: yuriy.baryshev@vntu.edu.ua

Yurii Baryshev — PhD. (Eng), Associated Professor of Information Protection Department, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : yuriy.baryshev@vntu.edu.ua