

АНАЛІЗ МЕТОДІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТИПУ GRAY BOX

Вінницький національний технічний університет;

Анотація

У дослідженні розглянуті методи, переваги, виклики та практичні застосування тестування сірого ящика. На основі синтезу академічної літератури та галузевих практик надається всебічний аналіз того, як тестування типу сірого ящика може покращити кіберзахист та відповідати сучасним потребам у розробці.

Ключові слова: тестування на проникнення, Gray Box, вразливості, автоматизація тестування

Abstract

This thesis explores the methodologies, benefits, challenges, and practical applications of gray box penetration testing. By synthesizing scholarly literature and industry practices, the thesis provides a comprehensive analysis of how gray box testing can improve cybersecurity defenses while addressing the nuanced needs of modern development cycles.

Keywords: penetration testing, Gray Box, vulnerabilities, automation of testing.

Вступ

Тестування на проникнення, також відоме як етичний хакінг, є проактивним підходом до ідентифікації та усунення вразливостей в ІТ-системах. Це процес симуляції дій зловмисного атакуючого для пошуку потенційних слабких місць. Тестування на проникнення можна поділити на три основні типи: black box (чорний ящик), white box (білий ящик) та gray box (сірий ящик). У той час як black box testing імітує зовнішнього нападника без внутрішнього доступу, а white box testing дозволяє повний доступ до системи, gray box testing забезпечує частковий доступ, що дає змогу моделювати перспективу нападника зі середнім рівнем привілеїв [1].

Gray box testing стає дедалі актуальнішим у сучасному світі кібербезпеки через складність і взаємопов'язаність систем. Завдяки обмеженому погляду на внутрішні механізми, такі як вихідний код, схема бази даних чи ключові конфігурації, цей підхід ефективно оцінює як зовнішні вразливості, так і слабкі місця, спричинені неправильною реалізацією внутрішніх механізмів [2]. Ця теза досліджує методології, що використовуються під час тестування gray box, практичні переваги та аналізує результати, яких можна досягти.

Аналіз

Методології сірого ящика поєднують елементи тестування білого та чорного ящиків. Тестувальникам надається часткова інформація про систему, як-от дані для входу в систему, схеми архітектури або обмежений доступ до внутрішнього вихідного коду. Використовуючи ці дані, вони моделюють перспективу нападника зі середнім рівнем доступу, зберігаючи критичний зовнішній погляд. Нижче наведено основні методології, що застосовуються в тестуванні на проникнення типу сірого ящика.

1) Етап передтестової підготовки. На цьому етапі визначається обсяг та збір інформації та налаштування середовища тестування [3].

2) Етап оцінки. Основні тестувальні операції спрямовані на ідентифікацію вразливостей за допомогою специфічних технік сірого ящика, а саме: статичний аналіз коду (обмежений доступ до вихідного коду дозволяє тестувальникам проводити статичний аналіз і виявляти помилки, такі як уразливість до SQL-ін'єкцій, неповна валідація даних чи застосування слабких методів шифрування), динамічний аналіз коду (завдяки інтерактивній роботі з додатком чи системою у ролі "привілейованого аутсайдера" тестувальники спостерігають її поведінку під час виконання. Вони шукають слабкі місця в механізмах аутентифікації, небезпечні сесійні куки та вразливість до проходження шляхів), тестування API (тестування сірого ящика дозволяє перевіряти як публічні API, так і напівприватні API, доступ до яких має автентифікований користувач, з метою виявлення

неправильного контролю доступу) [4], ескалация привілеїв через обліковий запис (використовуючи часткові облікові дані, тестувальники намагаються отримати доступ до заборонених ресурсів чи зловживати наданими правами. Наприклад, вони можуть підвищити повноваження від рівня звичайного користувача до адміністратора через помилки логіки), ін'єкції та "фаззинг" (тестувальники намагаються експлуатувати загальні вразливості, такі як SQL-ін'єкції чи міжсайтові скрипти (XSS)). Використовуючи часткові дані про схеми бази даних, вони оптимізують ці атаки для досягнення ефективності) та перевірка конфігурації (аналіз логів, помилок виявлення слабких місць в конфігурації).

3) Етап написання звіту.

Висновки

Тестування на прокненість типу сірого ящика є важливим інструментом для організацій, які шукають збалансований та ефективний підхід до оцінки їхнього рівня безпеки. На відміну від методів чорного або білого ящиків, така методологія використовує часткові інсайдерські знання для досягнення реалістичного, але водночас глибокого аналізу вразливостей [5]. Завдяки балансуванню між знанням внутрішніх механізмів і зовнішнім оглядом цей підхід дозволяє знаходити критичні проблеми у налаштуваннях доступу, логіці додатків і конфігураціях.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. OWASP. (2022). OWASP Testing Guide: Penetration Testing for Applications. Отримано з <https://owasp.org>
2. Scarfone, K., Souppaya, M., & Hoffman, P. (2008). *Guide to Test, Analyze, and Secure Systems* (NIST Special Publication 800-115). National Institute of Standards and Technology.
3. Bishop, M. (2005). *Introduction to Computer Security*. Addison-Wesley.
4. Shevchenko, N., et al. (2018). *Threat Modeling: A Practical Guide*. IEEE Cybersecurity.
5. Anderson, R. J. (2021). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3-й випуск). Wiley.

Швець Владислав Вікторович — Performance Analyst Testing EPAM Systems, Inc.

Науковий керівник: **Войтович Олеся Петрівна** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail voytovych.vk@vntu.edu.ua

Shvets Vladyslav V. — Performance Analyst Testing EPAM Systems, Inc.

Supervisor: Voytovych Olesya P. — Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical