Курачинська А.Р., магістрантка, група КБм-22-1,
Науковий керівник: Єфіменко А. А., к.т.н., доц.,
завідувач кафедри комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»

МЕТОДОЛОГІЇ ТА МЕТОДИ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Дослідження тестування на проникнення інформаційних систем є надзвичайно актуальним питанням внаслідок розповсюдженості таких систем та подальшого проникнення інформаційних технологій у всі сфери життя людини. Зараз існує багато ризиків, що пов'язані з порушенням конфіденційності, цілісності, доступності даних. Висновки після тестування на проникнення та подальші заходи захисту запобігають економічній, фінансовій та іншим шкодам. Під час тестування виявляються і перевіряються уразливості системи, які можуть виникнути через програмні або технічні помилки, некоректні налаштування, дефекти роботи. Крім того, тестування дозволяє чітко продемонструвати актуальність виявлених вразливостей і значимість потенційної шкоди.

Тестування на проникнення – це тестування системи з точки зору зловмисника. Оцінюючи засоби контролю безпеки, пентестер повинен передбачати як люди, процеси і технології можуть бути використані для отримання несанкціонованого доступу до цінної інформації. Керівництво організації часто буває здивоване тим, що механізми безпеки, які вони вважали надійними, не є такими. Процес тестування можна розбити на п'ять етапів: планування та дослідження, сканування, отримання доступу, підтримування доступу, приховування слідів

На сьогоднішній день наявні різні методології та методи, які гарантують ефективне тестування на проникнення, що охоплює всі важливі аспекти. Усі методи тестування можна розділити на три групи: методи «чорної скриньки», методи «білої скриньки» і методи «сірої скриньки». Тестування методом «чорної скриньки» – це тестування, як функціональне, так і нефункціональне, що не передбачає знання внутрішнього устрою компонента або системи [1]. Даний метод тестування схожий на справжні атаки зловмисника, оскільки він демонструє як злочинець без знань про систему, зможе прицільно атакувати та отримувати конфіденційну інформацію. Тестування методом «білої скриньки» базується на аналізі внутрішньої структури об'єкта тестування [1]. Пентестер має можливість обирати вхідні значення, ґрунтуючись на знанні коду, який буде їх обробляти. Метод «білої скриньки» допомагає заощадити час і гроші, також він корисний для імітації цілеспрямованої атаки на певну систему з використанням якомога більшої кількості векторів атак [2]. Зазвичай такий тип перевірки використовується перед релізом нових додатків для виявлення та усунення вразливостей перш ніж вони потраплять до системи і нашкодять. Тестування методом «сірої скриньки» передбачає комбінацію всіх переваг і недоліків двох попередніх методів. Тобто ми знаємо лише частину внутрішньої структури програми. Наприклад, передбачається, що доступ до внутрішньої структури та алгоритмів програмного забезпечення створює найефективніші тестові випадки, але саме тестування виконується за допомогою методів чорної скриньки, а саме з точки зору користувача.

Для забезпечення найкращих результатів, незалежно від застосовуваних тестів на проникнення, випробувач повинен дотримуватися методології проведення тестування. Найвідомішими з них є: OOSSTMM, OWASP, NIST, PTEST. OSSTMM (Open-Source Security Testing Methodology Manual) є рецензованою експертною методологією виконання тестів та метрик безпеки [3]. OWASP (Open Web Application Security Project) – це стандарт, що розробляється та оновлюється спільнотою, яка стежить за останніми загрозами. Окрім вразливостей програми, він також стосується логічних помилок процесів. NIST (National Institute of Standards and Technology) надає конкретні рекомендації щодо тестування на проникнення, щоб допомогти пентестерам підвищити точність тестів. PTEST (Penetration Testing Execution Standards) – це методологія метою якої є створення всеосяжного та сучасного стандарту для тестування на проникнення, а також підвищення обізнаності серед бізнесу щодо того, чого очікувати від тестування. Вибір методології та методів тестування та подальше проведення тестування є важливими етапом підтримки високого рівня захищеності будь якої інформаційної системи.

Список використаних джерел

1. Olsen K., Posthuma M., Ulrich S. Certified Tester Foundation Level (CTFL) Syllabus 2018 v3.1.1 / Klaus Olsen, Meile Posthuma, Stephanie Ulrich: General Assembly of the ISTQB, 2019.- 93 с.
2. Types of Pen Testing: Black Box, White Box & Grey Box [Електронний ресурс] // The Redscan Team. – 2022. – Режим доступу до ресурсу: https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/.
3. Vacca J. Computer and Information Security Handbook 3rd Edition / John Vacca: Morgan Kaufmann, 2017. – 1280 с.