ДОСЛІДЖЕННЯ МЕТОДОЛОГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Яцюк О.О.
Науковий керівник – к.т.н., доц. Федюшин О.І.
Харківський національний університет радіоелектроніки
(61666, м. Харків, пр. Науки 14, каф. Безпеки інформаційних технологій,
тел. (057) 702-14-25, email: d_its@nure.ua)

The given work is dedicated to the overview of popular penetration testing methods. The tools and methods used by hackers to achieve their goals are changing and improving. The main purpose of penetration testing is helping companies to secure their information by preparing them with simulation of real attacks. Penetration testing doesn't have established standard to cover all types of tested applications. But there are many methodologies with their approaches and recommendations.

У наш час, коли інформаційні технології є досить звичним засобом взаємодії, а інформація – найцінніша валюта, завжди буде головним питання збереження та обробки цієї інформації.

Завжди є вразливі місця, які умовно можна поділити на дві групи: відомі та невідомі. Особливо небезпечною є друга група, які не мають готових та перевірених виправлень і рекомендацій для запобігання. Тому, проблема захисту інформації є досить необхідною.

Penetration testing (англ.– тестування на проникнення) згідно з [1] – є метод оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу). Цей процес включає активний аналіз системи з виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення.

Відсутність в такому масштабному процесі єдиного стандарту робить організацію, реалізацію, звітність і аналіз результатів досить складними задачами. Існує декілька методологій для проведення тестування на проникнення, які були розроблені різними органами та компаніями з кібербезпеки.

У цій роботі буде проведено огляд популярних методологій для тестування на проникнення. Але треба зазначити, що вони відрізняються в тій чи іншій мірі: починаючи з області використання і закінчуючи глобальним підходом до організації процесу.

Опис популярних методологій виглядає наступним чином (див. [2]):

1) OSSTMM. OSSTMM – це механізм, який використовується для визначення операційної безпеки цільової області. Це, по суті, вимірювання

захисту між активами, використовуючи формулу з методом та підходом для ідентифікації та категоризації засобів контролю (заходів безпеки) та обмежень (слабких сторін або вразливостей).

2) OWASP. Цей фреймворк забезпечує методологію тестування на проникнення додатків, яка може не тільки виявити вразливості, які часто зустрічаються в Інтернеті та мобільних додатках, але також виявити більш складні логічні недоліки, що виникають внаслідок небезпечної практики розробки.

3) NIST. На відміну від інших посібників з інформаційної безпеки, він пропонує більш конкретні вказівки для тестерів на проникнення. За допомогою цієї основи можна на гарантувати інформаційну безпеку в різних галузях, включаючи банківську, комунікаційну та енергетичну.

4) PTES. Дотримуючись цього стандарту тестування на проникнення, тестери якомога ближче знайомляться з організацією та їх технологічним контекстом, дозволяючи їм визначати найдосконаліші сценарії атак, які можна було б зробити. Сім етапів, передбачених цим стандартом, гарантують успішне випробування на проникнення, пропонуючи практичні рекомендації.

5) ISSAF. Ці набори стандартів дозволяють тестувальнику ретельно планувати та документувати кожен крок процедури випробування на проникнення, від планування та оцінки до звітування та знищення артефактів. Цей стандарт відповідає всім етапам процесу.

На даний момент не існує комплексної методології проведення даного виду тестування. Кожна з розглянутих в даній роботі методологій фокусується на певних питаннях, і як наслідок, при проведенні комплексного тестування на проникнення неможливо повністю опиратись лише на одну методологію. З нашої точки зору тут необхідно орієнтуватись на масштаби організації та цінність ресурсів, що зберігаються, а також часові характеристики для впровадження та використання тієї чи іншої методики.

Список використаної літератури:

1. Wikipedia [Електронний ресурс] – 2021. – Режим доступу до ресурсу: https://clck.ru/TV29f.

2. Top 5 Penetration Testing Methodologies and Standards [Електронний ресурс] – Режим доступу до ресурсу: https://www.vumetric.com/blog/top-penetration-testing-methodologies/.