ПЕНТЕСТ ДОСЛІДЖЕННЯ ЯК СЕРВІС

Юхименко В.І.
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 introduction to penetration testing methodologies. One of the most reliable ways of maintaining information security is regular conducting of penetration testing. The main objective of penetration testing is to identify security weaknesses by simulation of real attacks. The methodology of pentest research as a service offered to clients of cloud services and local computers is considered. One of the possible architectures is offered.

У наші дні, особливо після початку пандемії, все більше компаній, як старих, так і нових, пристосувались до віртуального керування їхніми діловими операціями та процесами. Зазвичай це передбачає включення нових та існуючих технологій у такі операції, які полегшують ведення бізнесу та підвищують прибутковість. Ці технології можуть бути у формі настільного програмного забезпечення, веб-додатків, мережевих додатків та конфігурацій. Однак ці технології можуть мати вразливі місця які відомі, але не були виправлені продавцями, що створює шлях для використання цих місць зловмисниками.

Встановлення методології тестування на проникнення набуває все більшого значення при розгляді безпеки даних у веб-додатках та при реалізації технології хмарних обчислень. Чим більше ми покладаємось на мережеві комунікації та хмарні системи даних, тим більше ми стаємо вразливими до потенційно шкідливих кібератак сторонніх сторін.

На сьогоднішній день активно розвивається методологія організації пентест дослідження як сервісу − Penetration Test as a Service (PTaaS), що була запропонована досить недавно. Метою даної роботи є аналіз запропонованої моделі її функціонування та визначення основних компонент для взаємодії.

Безперервне тестування на проникнення дозволяє клієнтам не тільки отримати захист периметра, але й можливість переглядати в реальному часі найбільш актуальну інформацію, яка їм потрібна, для прийняття найбільш точних і своєчасних рішень щодо усунення вразливостей.

У спеціальному інтерфейсі, який надає PTaaS, фахівці з охорони периметра матимуть постійний доступ до такої інформації в будь-який час, незалежно від того, проводиться в даний час перевірка на проникнення або вже завершена. На додаток до актуальних даних, ви часто також можете отримати доступ до повної бази знань, аналітики та порад щодо пом'якшення загроз безпеці від постачальників PTaaS, а також перевірки ефективності лікування вразливості. Запропонована архітектура системи

складається з центру пентест-операцій, де здійснюється планування, набору серверів інтеграції (на базі Docker та віртуальних машин), сервісів AWS та набору серверів для забезпечення безпосередньо сервісів моніторингу та пен тестування.

Інтеграція з хмарними провайдерами та локальною інфраструктурою дозволяє нам взаємопов'язані перетворення мережевих адрес, віртуальних IP-адрес та іншої важливої інформації, яка стосується вразливих систем.

Постійний моніторинг сховищ програм та інтеграція з інструментами конвеєру CI / CD дозволяє запускати та аналізувати статичне та динамічне (SAST / DAST) тестування безпеки додатків кожного разу, коли ви розгортаєте код.

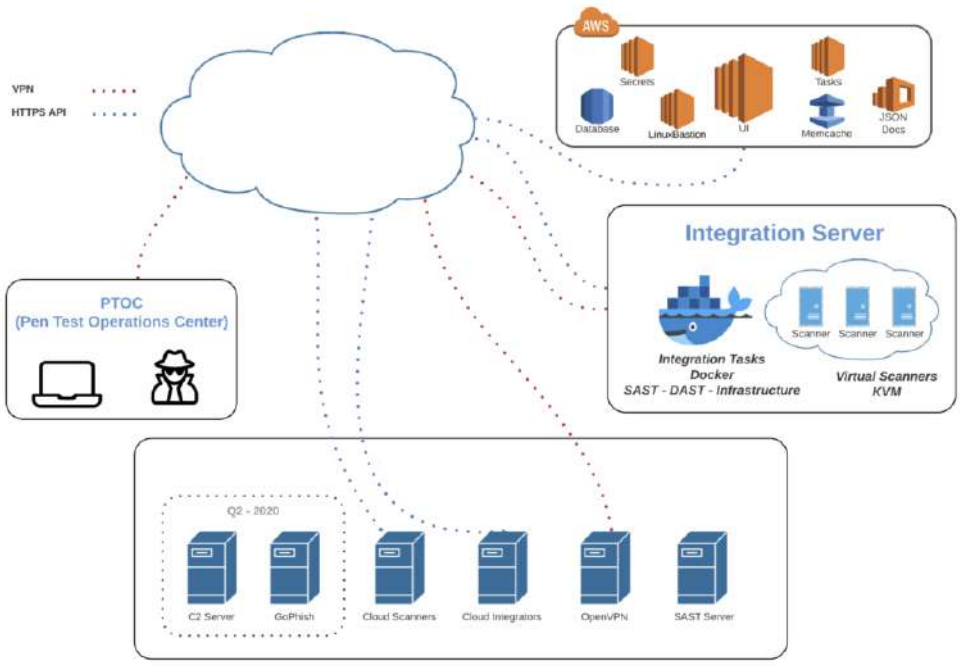

Рисунок 1 – Архітектура PTaaS

Метод надання послуг PTaaS добре працює для більшості компаній, незалежно від їх розміру. Найчастіше гнучкість платформ, що забезпечують PTaaS, дає можливість поєднувати все, що потрібно для захисту інформаційної системи клієнта, адже вона поєднує в собі постійний моніторинг безпеки, управління вразливістю, а також постійну підтримку та поради експертів.

Список використаної літератури:

1. What is pen test (penetration testing)? [Електронний ресурс] / [Linda Rosencrance, Puneet Mehta] // WhatIs.com. – 2018. – Режим доступу до ресурсу: https://searchsecurity.techtarget.com/definition/penetration-testing

2. Penetration Testing as a Service [Електронний ресурс] / [Raj Pagariya]. – Режим доступу до ресурсу: https://securityboulevard.com/2019 /04/penetration-testing-as-a-service/