УДК 004.056

В. Р. Коркошко
Л.М. Куперштейн

ПЛАТФОРМА ДЛЯ ПРОВЕДЕННЯ ЗМАГАНЬ З КІБЕРБЕЗПЕКИ

Вінницький національний технічний університет

Анотація
Досліджено та описано базові принципи роботи платформи для проведення змагань з кібербезпеки, а також вимоги яким вона повинна відповідати.
Ключові слова: кібербезпека, змагання, захоплення прапору.

Abstract
The basic principles of the platform for cybersecurity competitions and the requirements it must meet are studied.
Keywords: cybersecurity, competitions,capture the flag.

Вступ

У сучасному світі IT-системи знаходяться на піку свого розвитку і питання про їх кіберзахист стає більш актуальною з кожним днем. Для підготовки фахівців, які б забезпечували захист ресурсів, у багатьох навчальних структурах є і відповідна спеціальність - "кібербезпека", яка в своєму роді займається вивченням методів і практик захисту від зловмисних впливів.

Однією із важливих проблем підготовки майбутніх фахівців є мінімальні практичні навички в контексті пошуку і експлуатації різного роду вразливостей та загроз. Адже для того, щоб добре захищатися, потрібно розуміти як практично використовуються вразливості та проводяться кібератаки.

Для вирішення цієї проблеми пропонується створення спеціалізованої платформи для проведення змагань з кібербезпеки. Це дозволить чинним і майбутнім фахівцям застосовувати свої знання на практиці з певного роду емуляцією реальних додатків, а також додасть мотивації для отримання нових знань і більш глибокого розуміння практичного контексту роботи інформаційних систем.

Даного роду платформи як правило базуються на ідеї CTF (Capture the flag), що представляє собою командні змагання із захоплення прапора. Найбільш популярним реалізацією є "task-based" підхід, де команда учасників при виконанні завдання (наприклад, виявленні вразливості) отримує спеціальний прапор (як правило він має вигляд унікальної текстової мітки в контексті завдання), за яку команда отримує спеціальні бали. Кількість балів залежить від складності завдання та його категорії .

Базові категорії завдань, в контексті яких проводяться змагання з кібербезпеки [1]:

1. Web - завдання безпосередньо спрямовані на веб-безпеку (від пошуку типових xss-атак до file- або sql-ін'єкцій, з яких і випливає отримання несанкціонованого доступу до закритих для користувача ресурсів).
2. Crypto - пошук і експлуатація слабких місць криптографічних алгоритмів.
3. Stegano - отримання прихованої інформації.
4. Exploit - пошук вразливостей і їх експлуатація.

Результати дослідження

Реалізація платформи для проведення змагань з кібербезпеки передбачається у форматі веб-додатку, що дозволить прийняти участь та отримати доступ до завдань маючи пристрій з доступом до мережі Інтернет або засобами локальної мережі.

Основні вимоги для платформи:

- ізоляція вразливих застосунків від базового додатку;
- автоматизація розгортання вразливих додатків у якості завдань;
- можливість швидкого відновлення вразливих додатків у разі непрацездатності в наслідок дій учасників;
- генерація унікального прапора для кожної команди (щоб мінімізувати можливість отримання нечесних балів);

- логування всіх дій користувачів в контексті базової системи та вразливих додатків;

Спрощена структура платформи наведена на рис. 1.

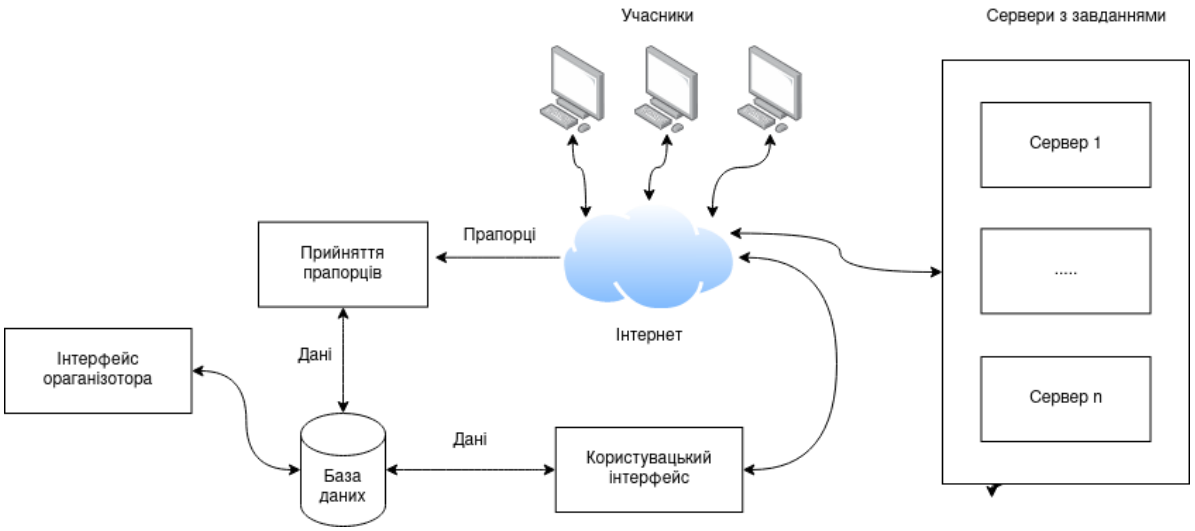

Рис 1. Спрощена структура платформи для проведення змагань з кібербезпеки

Головним компонентом для учасників являється користувацький інтерфейс, що реалізовується у вигляді веб-додатку. Безпосередньо в ньому розташовується список категорій та завдань з певним описанням та отримання доступу до них. Також інтерфейс відповідає за отримання та відображення актуальної статистики в процесі змагання: поточну кількість балів, кількість виконаних завдань, рейтинг команд за балами та список найбільше виконаних завдань. Перехід на сервер завдання виконується за спеціальної адресою, яка прив’язується до самого завдання. Сервіс прийняття прапорців відповідає за прийняття прапорців від учасників та їх приналежності до учасників, а також вказаного завдання. В базі даних зберігається основні дані про зареєстрованих учасників, загальна інформація про завдання та загальний стан процесу змагання. На серверах із завданнями розміщуються вразливі додатки.

Також в платформі присутній інтерфейс організатора, це саме те місце, де створюються категорії та задачі для них, а також події у вигляді змагання з можливістю вказання дати початку та завершення. Додатково в ньому присутня вся інформація (включаючи статистику) з можливістю повного контролю учасників (наприклад, блокування у випадку порушування правил змагання).

В специфіку дотримання оголошених раніше вимог для поточної платформи є доцільним розглянути варіант використання спеціалізованого інструменту з назвою Docker [2]. Це дозволяє упакувати різного роду додатки разом з його залежностями в спеціалізований контейнер. Цей підхід є більш ефективнішим в плані використання ресурсів системи, розмірів та швидкості розгортання.

Для досягнення унікальності прапорців планується їх генерування у реальному часі, тобто кожен з серверів з завданнями буде мати можливість ідентифікувати учасника за спеціальним токеном, після чого отримати його за допомогою спеціального API з основною системою у вигляді текстової мітки [3].

Для спрощеного логування всіх дій користувачів достатньо використовувати стандартні механізми реєстрації запитів до веб-сервера (наприклад, NGINX) [4]. Після чого в певний короткий інтервал часу виконувати передачу всіх журналів на інший сервер, щоб знову ж таки мінімізувати можливість їх спотворення.

Загальні етапи роботи із платформою:

- реєстрація учасників;
- учасники отримують доступ до відповідних завдань у вигляді карток, де безпосередньо вказуються адреси серверів з завданнями;

- учасник переходить на сервер з завданням і починає виконувати аудит вразливого додатку;
- знаходження прапорця учасником;
- підтвердження виконання завдання з вказанням знайденого прапорця та отримання балів;
- завершення змагання та підведення підсумків.

Висновки

Запропоновано узагальнену структурну схему платформи для проведення змагань з кібербезпеки. Описано принципи функціонування системи та основних її структурних компонентів. Реалізація та подальша експлуатація системи дозволить підвищити теоретичні знання та практичні навички фахівця з кібербезпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. CTF: Capture the Flag: веб-сайт. URL: https://xakep.ru/2016/06/14/ctf/ (дата звернення: 04.03.2021)
2. What is a Container? | Docker: веб-сайт. URL: https://www.docker.com/resources/what-container (дата звернення: 04.03.2021)
3. NGINX Docs | Configuring Logging: веб-сайт. URL: https://docs.nginx.com/nginx/admin-guide/monitoring/logging/ (дата звернення: 05.03.2021)
4. API: веб-сайт. URL: https://developer.mozilla.org/ru/docs/Glossary/API (дата звернення: 05.03.2021)

Коркошко Віктор Русланович – студент групи 1БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: victor.korkoshko@gmail.com

Куперштейн Леонід Михайлович — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Korkoshko Victor R. — Student of Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : victor.korkoshko@gmail.com

Kupershtein Leonid M. — PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com