Освітній потенціал CTF-змагань у структурі кіберполігонів для ЗВО

https://doi.org/10.31713/MCIT.2025.057

Сергій Бабич
Національний університет водного господарства та природокористування
Рівне, Україна
s.v.babych@nuwm.edu.ua

Богдан Слив'як
Національний університет водного господарства та природокористування
Рівне, Україна
b.v.slyviak@nuwm.edu.ua

Гліб Онищук
Національний університет водного господарства та природокористування
Рівне, Україна
h.o.onyshchuk@nuwm.edu.ua

Анотація **– у статті розглянуто потенціал використання ігровізації методикою Захоплення прапору (CTF) для збільшення ефективності навчання кібербезпеці як інноваційного освітнього методу. Запропоновано використання кіберполігону в лабораторіях ВНЗ як місця розміщення нетипових завдань з кібербезпеки чи моделювання реальних завдань на підставі отриманого раніше досвіду.**

Даний підхід має змогу запропонувати навички та знання для виявлення, запобігання та реагування на кіберзагрози практичного характеру, що є найбільш вразливою стороною навчального процесу з кібербезпеки в ЗВО.

Ключові слова **– кібербезпека, CTF, навчання, кіберполігон, ігровізація в ЗВО.**

I. ВСТУП

Актуальність кібербезпеки важко переоцінити, навіть якщо не звертати увагу на більше десяти років війни, та, відповідно, кібертерактів в Україні [1,2] – питання захисту в кіберсередовищі стає все більш актуальною, адже, згідно з прогнозами, вартість кіберзлочинів досягнуло 8 трильйонів у 2023 році і зросло до 10,5 трильйонів до 2025 року, як зазначено у звіті [3].

З огляду на стрімке зростання кіберзлочинів [5] та постійний тиск на кіберпростір України загалом [1, 2], важливо інвестувати в освіту, зокрема в практичні навички з кібербезпеки студентів ЗВО.

В останні роки особливо різко стає зрозуміло, чому традиційні методи навчання можуть бути не такими ефективними, як в інших галузях [6]. Лекції та практичні (лабораторні) роботи не завжди мають змогу продемонструвати реальні ситуації, до яких має бути готовий студент після закінчення навчання.

Інтегрування CTF, як методики навчання, пропонує доповнити теоретичні знання створенням та подальшим проходженням завдань, виключно практичного характеру, а також створенням умов конкуренції та ігровізації, як мотивацій до виконання цих завдань та навчання в сфері кібербезпеки загалом (що стосується і дотичних предметів, для прикладу – комп'ютерних мереж). Окрім того, спільні інтереси ігровізації значно збільшують ймовірність обговорення отриманого досвіду з CTF та дотичних тем загалом.

II. ЗАГАЛЬНА ЧАСТИНА

«Capture the Flag» (CTF) – це тип змагань з кібербезпеки, в яких учасники мають знайти та використати вразливі місця в комп'ютерній системі чи мережі. Дані змагання можуть бути розроблені так, аби імітувати реальні ситуації з кібербезпеки, або сценарії реальних кібервтручань. Ці завдання можна розглядати як кіберголоволомки, що можуть відображати кіберкультуру чи інші культурні надбання, котрі будуть зрозумілі молоді та можуть сприяти ігровізації навчального процесу.

Ціль CTF завдань – захоплення прапора, особливого рядка інформації, з яким знайомлять учасників до початку змагань, серед великої кількості даних, що імітують реальні сервіси, мережу, тощо; знаходження всієї прихованої інформації раніше за інших учасників. CTF-прапор може бути прихований у файлах, або конфіденційній інформації, доступ до якої можна отримати лише шляхом використання деяких вразливостей у системі (що може слугувати «ключем» та вимагати відповідних знань). Зазвичай існує кілька способів вирішення конкретного завдання.

Змагання CTF варто використовувати для навчання та підготовки, а також для оцінки та поліпшення безпеки реальних систем шляхом симуляції на кіберполігоні (що є значно безпечнішим, ніж подібний стрес-тест робити «наживо»).

Окремо варто зазначити моделювання, на кіберполігоні, ситуацій реальних кіберзлочинів на

підставі розслідування кіберінцидентів, що дає змогу отримати більше досвіду з подібних ситуацій (наприклад, написання звіту з кібербезпеки після тесту на проникнення для компанії або вирішення завдань з бінарної експлуатації, що включають 0-день), аніж просто про них прочитати, що може покращити ефективність розслідування, адже під час змагань CTF можуть бути виявлені вразливості 0-days [7, 8].

Змагання CTF та використання кіберполігону, як інструмент та методика, може бути корисним для навчання в галузі кібербезпеки [9, 10], оскільки забезпечує безпечне та контрольоване середовище, в якому учасники можуть отримати практичний досвід у виявленні та використанні вразливостей, що є необхідним для розвитку практичних навичок у галузі кібербезпеки. Симуляції, лабораторні роботи та навчання на основі сценаріїв можуть бути ефективними практичними підходами.

Змагання можуть варіюватися від місцевих заходів, що проводяться в університетах або хакатонах, до міжнародних змагань. У вересні 2025 року, в Україні провели перший національний чемпіонат з технологічного спорту в дисципліні CTF [3]. Іншими, міжнародними прикладам слугують DEF CON CTF [11], щорічне змагання в Лас-Вегасі під час найвідомішої в світі конференції з кібербезпеки, Google CTF, Codegate CTF, що проводиться щорічно в Південній Кореї, Pwn2Own, де учасники повинні знайти вразливості 0-days і проводиться двічі на рік на конференції з безпеки CanSecWest. Аби бути в курсі подій CTF, а також рейтингу змагань і команд по всьому світу, можна відвідати вебсайт «CTFtime» [12].

CTF-змагання можна розділити на різні класи: Jeopardy, Attack-and-Defense (A/D), King of the Hill (KotH), Boot2Root та змішаний стиль.

Jeopardy CTF: серія завдань, складність яких поступово зростає (а разом з нею і кількість балів), розділених на такі категорії, як веб, бінарна експлуатація, криптографія тощо. Після закінчення відведеного часу перемагають учасники з найвищим балом.

A/D: кожній команді надається сервер з певною кількістю вразливих служб, які періодично використовуються ботом. Цей бот генерує та записує прапори на кожному сервері. Учасники повинні виправити вразливості своїх служб, не порушуючи їх роботи (захист), та експлуатувати ті самі вразливості в інших командах (атака). Остаточний результат обчислюється шляхом підрахунку кількості прапорів, викрадених кожною командою, часу доступності сервісу, тощо.

«Король гори»: команди змагаються за контроль над вразливою системою або мережею та намагаються утримати контроль якомога довше. Перемагає команда, яка утримує контроль найдовше.

CTF boot2root: командам надаються вразливі віртуальні машини. Метою є отримання прав адміністратора.

У змішаній категорії розглядаються всі інші типи CTF-змагань. Прикладами можуть бути змагання, в яких всі завдання беруться з реальних програм; як уже згадувалося, можуть бути змагання з метою пошуку 0-денних вразливостей.

Інші CTF можуть включати фізичні пристрої, такі як розумні автомобілі або супутники. Використання CTF для навчання кібербезпеці може бути розумним кроком, оскільки воно використовує переваги ігрофікації навчального процесу [13].

Навчання кібербезпеці за допомогою змагань CTF може підвищити зацікавленість студентів і, отже, покращити загальний навчальний процес [14]. Проте використання завдань CTF як засобу для введення або просування в кібербезпеці має недолік, оскільки не є достатньо гнучким, щоб дозволити його використання для широкого кола учасників.

Насправді завдання часто далекі від реальних випадків або сильно різняться за складністю вирішення. З цих причин варто звернути увагу на модель навчання кібербезпеці, де групи студентів кидають виклик один одному, створюючи завдання CTF.

Поділ студентів на групи приблизно однакового розміру та подальша співпраця для створення завдань на обрані теми, які суворо пов'язані з навчальними цілями, специфічними для кожного курсу. Наступним кроком, завдання повинні бути запропоновані всім іншим групам або лише їх підгрупі, що дасть можливість контролювати вибір тем та груп студентів. Використовуючи запропоновану методику навчання, очікується зріст зацікавленості з боку студентів, що має призвести до кращих результатів у підсумковій оцінці, а також значно покращити якість освітнього процесу по даній тематиці та суміжними предметами.

III. КІБЕРПОЛІГОН

З метою підтримки впровадження запропонованого методу, необхідна платформа, на якій можна масштабовано реалізувати необхідні завдання та сам процес.

Варто зазначити, що в Інтернеті існує безліч ресурсів з навчання CTF, а також шпаргалки, фрагменти коду та навчальні платформи. Деякі відомі приклади: «TryHackMe» та «HackTheBox», де існують як безкоштовні, так і платні плани. Обидві платформи представляють теми кібербезпеки у вигляді серії лекцій та відповідних завдань. Існують також платформи, присвячені конкретним категоріям, наприклад, «exploit.education» і «pwn.college» для категорії бінарних експлойтів та «cryptohack» для криптовалют.

Пропонується підхід (зображено на рис. 1), що має вигляд лабораторії ЗВО з елементами базової структури платформи CTF: домашня сторінка, що містить загальні правила та вказівки; таблиця результатів, де відображається поточний рейтинг учасників, а також хто вирішив яке завдання; завдання, розділені за категоріями та впорядковані за балами або часом випуску. Крім того, кожна команда

матиме особистий цифровий простір, де можна буде завантажувати створені завдання та вибирати команди, яким будуть поставлені завдання. Важливо, також, сформувати умови для зручних offline-занять з пріоритетним використанням персональних комп'ютерів (ноутбуків) в цілях мотивації завчасної підготовки та додаткової роботи з інструментами, що використовуються в даних заходах.

Нарешті, буде присутній «режим історії», що дозволить кожному учаснику пережити історію та вирішити загадки, використовуючи навички кібербезпеки, набуті під час гри.

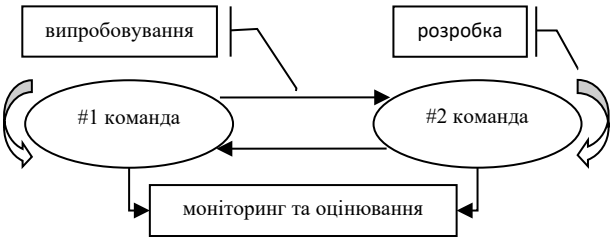

Рисунок 1. Схема для двох груп, які створюють завдання CTF, кидають виклик одна одній, а результати демонструються в аудиторії на загал

III. ВИСНОВКИ

Навчання студентів ЗВО з використанням новітніх методик, зокрема запропонованої, разом із лекційним навантаженням та платформою для створення, обміном та виконанням завдань CTF – кіберполігоном, з вивчених на лекціях тем, має продемонструвати значно кращу якість знань наприкінці курсу та компетентність студентів загалом.

Крім того, отримані дані стануть основою для відповідних змін як в навчальних матеріалах так й в подальших завданнях та симуляціях.

Запропонована інноваційна методологія, а також платформа, можуть бути застосовані в різних контекстах, починаючи від вступного рівня освіти в галузі кібербезпеки до курсів університетського рівня та курсів підвищення кваліфікації на професійному рівні галузі.

Така робота ЗВО зі студентами в навчальному процесі сприятиме інтеграції даної концепції навчання з іншими архітектурами (кіберполігонами інших ЗВО) для передачі знань у галузі кібербезпеки [14] та з існуючими методологічними та технологічними рамками для навчання («Tryhackme», «Hackthebox», тощо).

ЛІТЕРАТУРА

[1] European Parliamentary Research Service. Digital euro: Central bank digital currencies and the future of money. Briefing, PE 733.549, European Parliament, 2022. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf

[2] Aspen Institute Kyiv. Український ринок кібербезпеки зріс у чотири рази за вісім років [Електронний ресурс] // Aspen Institute Kyiv. – 2023. – Режим доступу: https://aspeninstitutekyiv.org/ukrainskyi-rynok-kiberbezpeky-zris-u-chotyry-razy-za-visim-rokiv/

[3] Рівненська обласна державна адміністрація. Команда з Рівненщини – у ТОП-5 першого чемпіонату України з кіберспорту CTF [Електронний ресурс] // Офіційний вебсайт Рівненської ОДА. – 2024. – Режим доступу: https://www.rv.gov.ua/news/komanda-z-rivnenshchyny-u-top-5-pershoho-chempionatu-ukrainy-z-kibersportu-ctf

[4] Cybersecurity Ventures. 2023 Official Cybercrime Report / Sponsored by eSentire [Електронний ресурс] // eSentire. – 2023. – Режим доступу: https://www.esentire.com/resources/library/2022-official-cybercrime-report

[5] IBM Security.** Cost of a Data Breach Report 2025 [Електронний ресурс] // IBM. – 2025. – Режим доступу: https://www.ibm.com/reports/data-breach

[6] A. McGettrick, Toward effective cybersecurity education, IEEE Security & Privacy 11 (2013) 66–68.

[7] Wallarm, Php remote code execution 0-day discovered in real world ctf exercise, https://lab.wallarm.com/php-remote-code-execution-0-day-discovered-in-real-world-ctf-exercise/, 2019.

[8] NIST, Php remote code execution 0-day discovered in real world ctf exercise, https://nvd.nist.gov/vuln/detail/CVE-2022-4349, 2022.

[9] E. Trickel, F. Disperati, E. Gustafson, F. Kalantari, M. Mabey, N. Tiwari, Y. Safaei, A. Doupé, G. Vigna, Shell we play a game? ctf-as-a-service for security education., in: ASE@ USENIX Security Symposium, 2017.

[10] A.Mansurov, et al., A ctf-based approach in information security education: an extracurricular activity in teaching students at altai state university, russia, Modern Applied Science 10 (2016) 159.

[11] C. Cowan, S. Arnold, S. Beattie, C. Wright, J. Viega, Defcon capture the flag: Defending vulnerable code from intense attack, in: Proceedings DARPA Information Survivability Conference and Exposition, volume 1, IEEE, 2003, pp. 120–129.

[12] CTFtime.org. Платформа для відстеження та участі у змаганнях з кібербезпеки (CTF) [Електронний ресурс] // CTFtime.org. – Режим доступу: https://ctftime.org/

[13] G. Kiryakova, N. Angelova, L. Yordanova, Gamification in education, in: Proceedings of 9th international Balkan education and science conference, volume 1, 2014, pp. 679–684.

[14] K. Boopathi, S. Sreejith, A. Bithin, Learning cyber security through gamification, Indian Journal of Science and Technology 8 (2015) 642–649.