Нестеров В.Ю., магістрант,
Єфіменко А.А., к.т.н., доцент,
Державний університет «Житомирська політехніка»

АЛГОРИТМ РОЗГОРТАННЯ ПЛАТФОРМИ ДЛЯ ПРОВЕДЕННЯ НАВЧАЛЬНИХ КІБЕРБЕЗПЕКОВИХ ДОСЛІДЖЕНЬ ЗА НАПРЯМОМ PENETRATION TESTING У ФОРМАТІ CTF

У сучасних умовах зростання кібератак питання захисту інформації стає надзвичайно актуальним. Для забезпечення надійної кібербезпеки важливо застосовувати ефективні методи навчання та перевірки навичок виявлення й усунення вразливостей. Одним із найкорисніших форматів є CTF, який розвиває практичні навички студентів. Для цього потрібна платформа, яка дозволить їм проводити дослідження та вирішувати реальні завдання з кібербезпеки.

Метою цього дослідження є розробка алгоритму для розгортання, налаштування та наповнення платформи для проведення навчальних кібербезпекових досліджень за напрямом Penetration Testing у форматі CTF. Алгоритм включає етапи, необхідні для ефективного впровадження платформи, створення завдань та налаштування середовища, що дасть змогу студентам застосовувати теоретичні знання й удосконалювати практичні навички.

CTF (Capture the flag) – це змагання в галузі кібербезпеки, де учасники або команди вирішують завдання, пов'язані з безпекою комп'ютерних систем, з метою знайти прапор (flag) заздалегідь визначений рядок символів, що підтверджує успішну експлуатацію вразливості та розв'язання завдання [1].

Розгортання ефективної платформи для проведення CTF передбачає виконання кількох етапів:

Огляд наявних рішень для розгортання платформи: На першому етапі необхідно розглянути популярні рішення та обрати найбільш підходяще, виходячи з конкретних вимог та потреб. Сьогодні найпопулярнішим рішенням для розгортання платформи є CTFd;

Огляд наявних ресурсів готових VM-жертв: На другому етапі необхідно визначитися з вибором VM-жертв, на основі яких будуть створюватися завдання для платформи. Важливо, щоб ці VM-жертви були безкоштовними та включали різноманітні вразливості. Одним із найпопулярніших ресурсів готових VM-жертв сьогодні є VulnHub;

Мережева інфраструктура: На третьому етапі необхідно спроектувати та створити надійну мережеву інфраструктуру для коректного функціонування платформи. Важливо передбачити підмережі для клієнтів, сервера та VM-жертв. Оптимальним вибором для мережевого обладнання є пристрої Cisco, зокрема маршрутизатори та комутатори. Усі пристрої в мережі слід з'єднувати за допомогою технологій Ethernet та Fast Ethernet;

Розгортання та налаштування: На четвертому етапі необхідно обрати операційну систему для сервера, зазвичай це Ubuntu. Далі потрібно вибрати VM-жертви, на основі яких створюватимуться завдання для платформи. Після встановлення операційної системи на сервер важливо інсталювати Docker. Наступним кроком є розгортання платформи на базі рішення CTFd. Після успішного розгортання платформи її слід налаштувати. Фінальним кроком на цьому етапі є встановлення OpenVPN для зв'язку з майбутніми VM-жертвами;

Наповнення платформи завданнями: На п'ятому етапі необхідно створити завдання на платформі для кожної з попередньо обраних VM-жертв. Найоптимальніший підхід це створити серію завдань, яка матиме певну кількість балів, поступово ускладнюватиметься та міститиме підказки для допомоги у вирішенні;

Тестування роботи мережі та функціоналу платформи: На шостому (фінальному) етапі необхідно провести тестування встановлених налаштувань в мережі та функціонування платформи.

Запропонований алгоритм розгортання платформи для проведення навчальних кібербезпекових досліджень за напрямом Penetration Testing у форматі CTF поєднує теоретичні та практичні аспекти. Теоретично він грунтується на системному підході до створення та налаштування інфраструктури, що враховує безпеку, зручність і ефективність. Практично алгоритм реалізує розгортання платформи, що надає студентам можливість працювати з реальними кіберзагрозами, покращуючи навички виявлення та усунення вразливостей через вирішення складних задач з інформаційної безпеки.

У доповіді буде представлено використання наведеного вище алгоритму розгортання платформи для проведення навчальних кібербезпекових досліджень за напрямом Penetration Testing у форматі CTF. Перспективи подальших досліджень спрямовані на вдосконалення інфраструктури платформи, розширення кількості та складності завдань.

Список використаних джерел

1. Sancheti S. CTF and its Types For Beginners !. Medium. URL: https://medium.com/@007ssancheti/ctf-and-its-types-for-beginners-aeb9904e9df (date of access: 02.12.2024).