

Лабораторна робота. Вразливості систем кібербезпеки

Цілі та задачі

Навчитися визначати типи вразливостей систем кібербезпеки.

Довідкова інформація / Сценарій

Класифікація вразливостей систем безпеки:

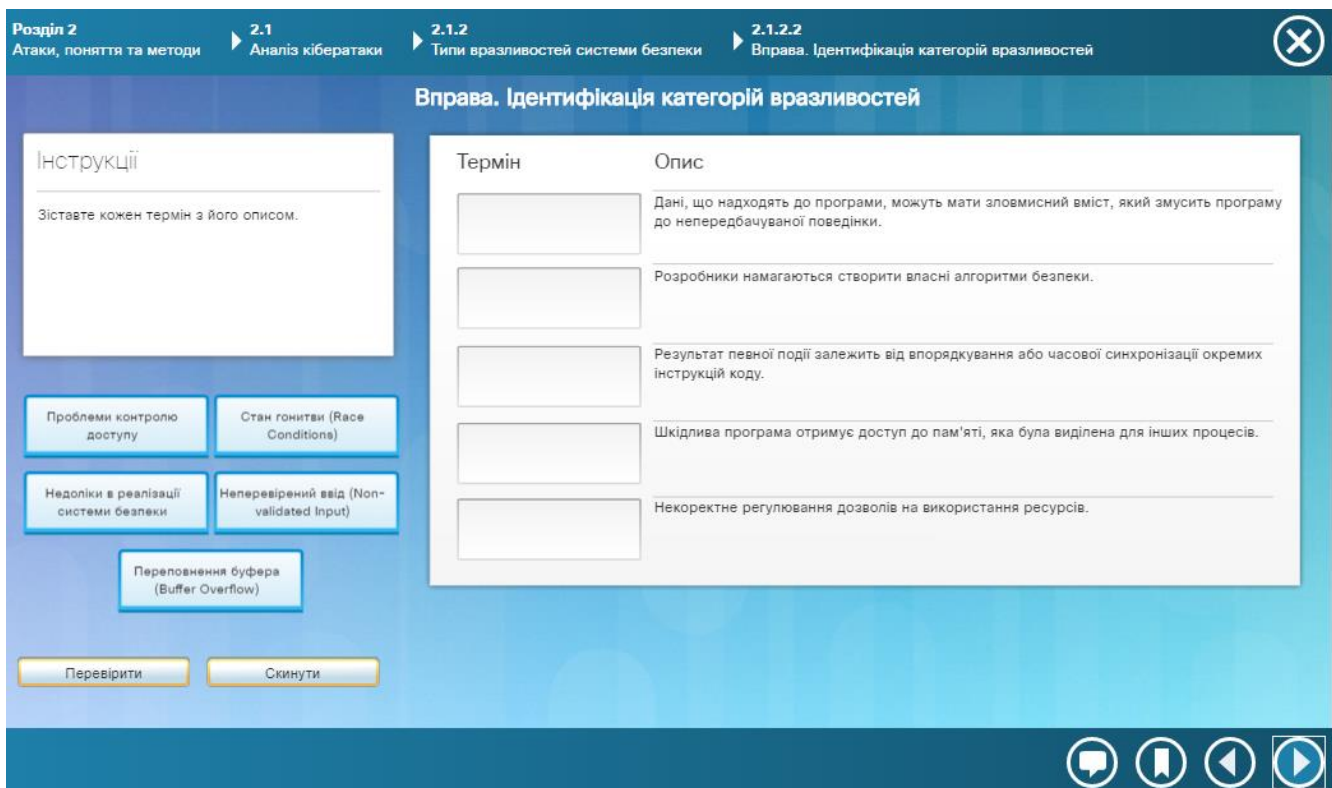
- Переповнення буфера (Buffer overflow)
- Непереверені вхідні дані (Non-validated input)
- Стан гонитви (Race conditions)
- Недоліки реалізації системи безпеки (Weaknesses in security practices)
- Проблеми контролю доступу (Access-control problems)

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету.

Дослідження вразливостей систем безпеки

1. Виконайте вправу:



The screenshot shows a lab interface with a breadcrumb trail: Розділ 2 (Атаки, поняття та методи) > 2.1 (Аналіз кібератаки) > 2.1.2 (Типи вразливостей системи безпеки) > 2.1.2.2 (Вправа. Ідентифікація категорій вразливостей). The main title is 'Вправа. Ідентифікація категорій вразливостей'. On the left, there is an 'Інструкції' section with the text 'Зіставте кожен термін з його описом.' Below it are five buttons: 'Проблеми контролю доступу', 'Стан гонитви (Race Conditions)', 'Недоліки в реалізації системи безпеки', 'Непереверений ввід (Non-validated Input)', and 'Переповнення буфера (Buffer Overflow)'. At the bottom left are 'Перевірити' and 'Скинути' buttons. On the right, there is a table with two columns: 'Термін' and 'Опис'. The table contains five rows, each with an empty input field in the 'Термін' column and a description in the 'Опис' column.

Термін	Опис
<input type="text"/>	Дані, що надходять до програми, можуть мати зловмисний вміст, який змусить програму до непередбачуваної поведінки.
<input type="text"/>	Розробники намагаються створити власні алгоритми безпеки.
<input type="text"/>	Результат певної події залежить від впорядкування або часової синхронізації окремих інструкцій коду.
<input type="text"/>	Шкідлива програма отримує доступ до пам'яті, яка була виділена для інших процесів.
<input type="text"/>	Некоректне регулювання дозволів на використання ресурсів.

2. Виконайте вправу:

Вправа. Визначення типів шкідливих програм

Визначте типи шкідливого ПЗ

Зістаєте кожен термін з його описом.

Мітмо	Бот
Вірус	Scareware (псевдодантивірус)
Троянський кінь	Adware (рекламне ПЗ)
Ransomware (програми-вимагачі)	Worm (хробак)
Руткіт	Шлигунське ПЗ

Термін	Опис
<input type="text"/>	Шкідливе ПЗ, призначене для автоматичного виконання дій, зазвичай, в Інтернеті.
<input type="text"/>	Зловмисне ПЗ, призначене для блокування комп'ютерної системи або даних до моменту отримання викупу.
<input type="text"/>	Зловмисне ПЗ, призначене для створення змін у операційній системі з метою створення чорного ходу (backdoor).
<input type="text"/>	Зловмисне ПЗ, яке часто розповсюджується разом з легальними програмами та призначене для відстеження активності користувача.
<input type="text"/>	Шкідливий виконуваний код, який додається до інших виконуваних файлів, часто легальних програм.
<input type="text"/>	Зловмисне ПЗ, яке здійснює шкідливі дії під виглядом бажаної операції.
<input type="text"/>	Шкідлива програма, яка призначена для автоматичного поширення реклами. Іноді розповсюджується в комплекті з іншим програмним забезпеченням.
<input type="text"/>	Зловмисне ПЗ, яке використовується для отримання контролю над мобільним пристроєм.
<input type="text"/>	Шкідливе ПЗ, яке переконує користувача здійснити конкретну дію, використовуючи його страх.
<input type="text"/>	Шкідливий код, який самостійно клонує себе, використовуючи вразливості в мережах.

3. Опишіть дії для зменшення наслідків вразливості систем безпеки

Контрольні питання:

1. Що таке вразливість системи безпеки?
2. Яка з вразливостей найбільш небезпечна на ваш погляд і чому?