Основи інформаційної безпеки

ПЗ №5

Тема: “Безпечне зберігання паролів”

Підготував:

Студент групи МІТ-21

Денісов Ілля

Способи зберігання паролів:

1) Зберігання паролів у відкритому вигляді

Небезпечний метод

2) Шифрування паролів

Використовування секретного ключа безпечно.

3) Хешування паролів

Шахраї можуть скористатися атакою з використанням райдужних таблиць.

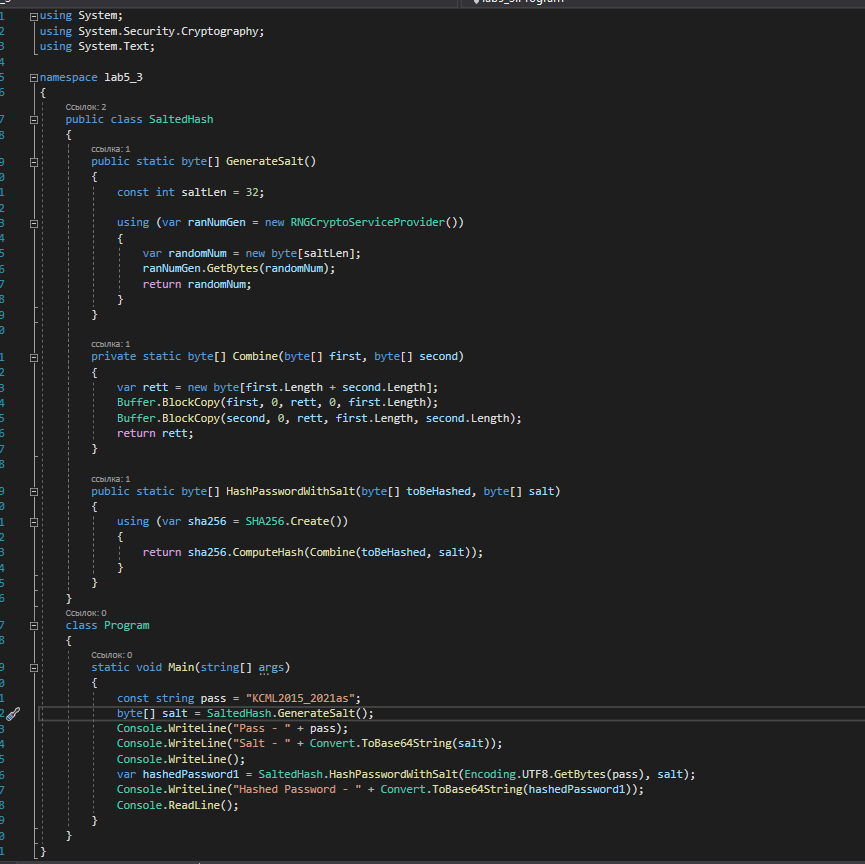
4) Використання хешу та солі для зберігання пароля

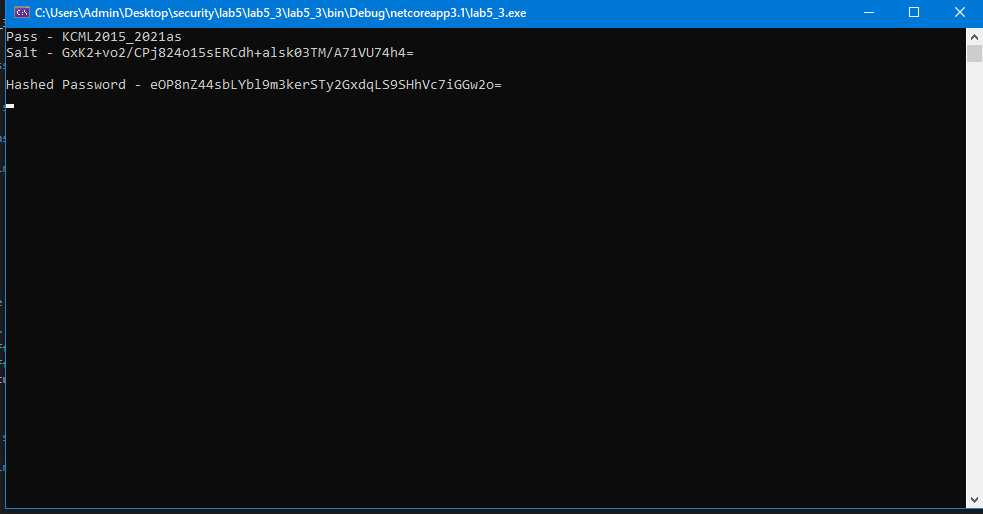
Так як це випадковий набір цифр, то кожен раз хеш буде змінюватися.

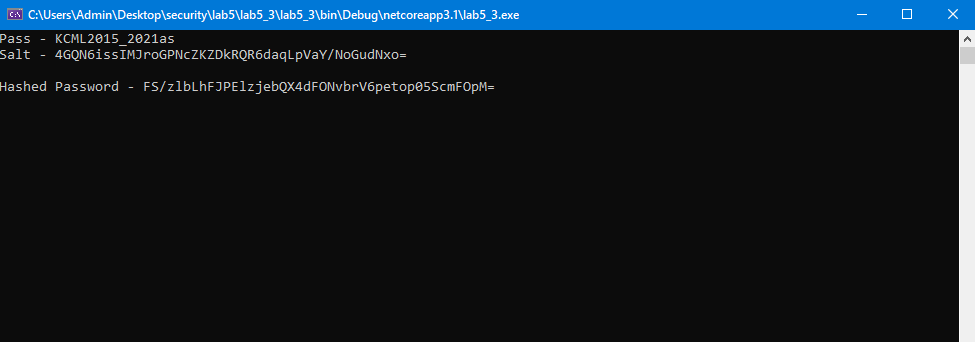
5) Використання спеціальних функцій

Ітерації повторюють хешування пароля декілька разів

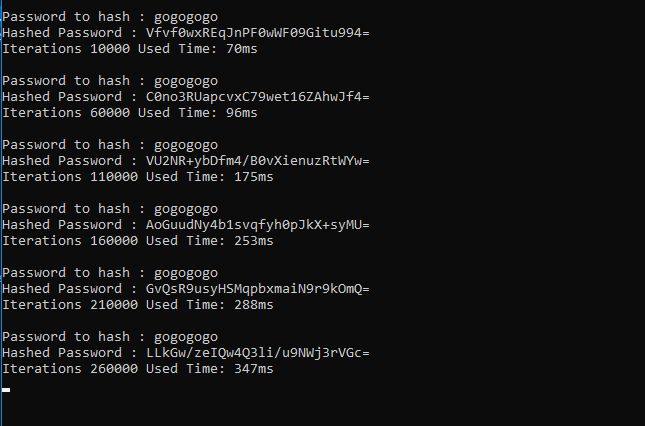
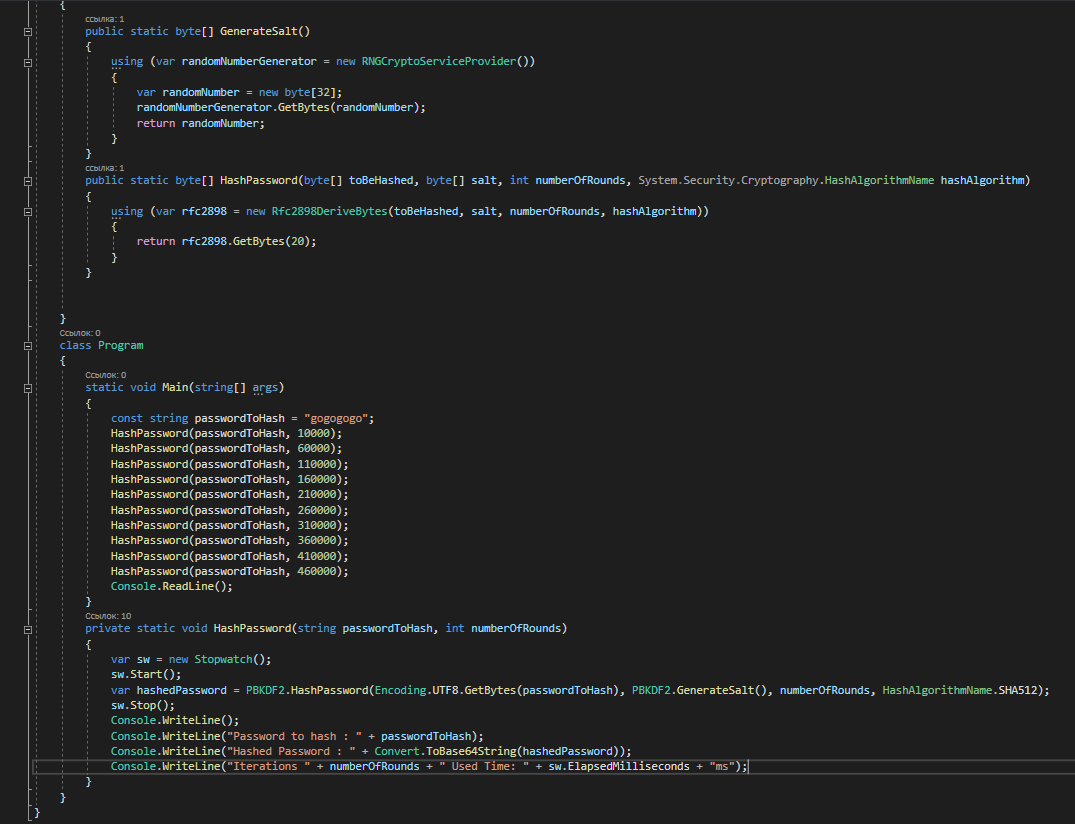
Завдання 3







Висновок: через те, що ми використовуємо хешування з сіллю, кожен раз маємо інший варіант хешу пароля.

Завдання 4

Висновок: у ході лр я зрозумів як генерувати випадкову сіль. Навчився хешувати декілька разів вже захешований пароль разом із сіллю й визначив час, який витрачається на певну кількість таких ітерацій. Навчився хешувати паролі різними алгоритмами хешування разом із сіллю.