ЛАБОРАТОРНА РОБОТА 4

РЕВЕРС ІНЖИНІРИНГ

**1.1 Мета роботи**

− виконати реверс інжиніринг програми з метою вивчення її поведінки

**1.2 Завдання на роботу**

Задачею на лабораторну роботу є виконання реверс інжинірингу бінарного файлу “sys\_prog\_lab2\_your-nickname” в Ghidra.

**1.3 Хід виконання**

Першим кроком необхідно завантажити генератор завдання, з платформи Github (для Linux ОС):

<https://github.com/armymotion/cpnu_sysprog_2024/tree/main/lab4_task>

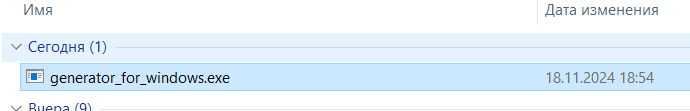


Рис.1 – Завантажений .exe файл

Після чого виконаємо запуск генератора, для створення sys\_prog\_lab2 файлу, як проілюстровано на (рис. 2)

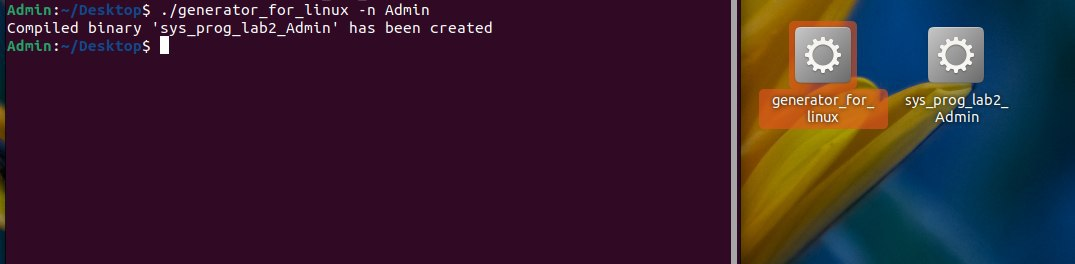


Рис. 2 – Запуст виконуваного файлу «generation\_for\_linux»

Наступним кроком є встановлення Ghidra, мною було використано наступне джерело : <https://www.youtube.com/watch?v=Es3ebWUBiqc>. Після успішного встановлення, запустимо Ghidra та створимо новий проєкт (рис. 3)

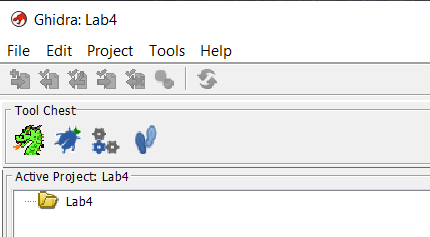


Рис. 3 - Новий проект

Далі завантажемо файл «sys\_prog\_lab2» в Ghidra для виконання інжинірингу (рис. 4)

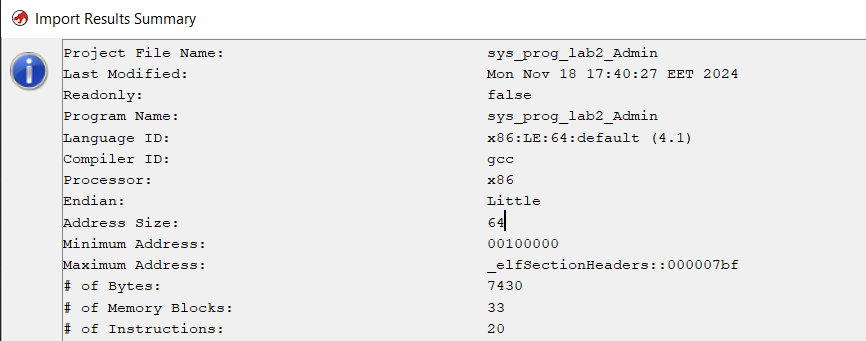


Рис. 4 - Додавання файлу до проекту для інжинірингу

Після напискання на іконку дракона, отримуємо інжиніринг та декомпозицію на мові С з правого боку (рис. 5)

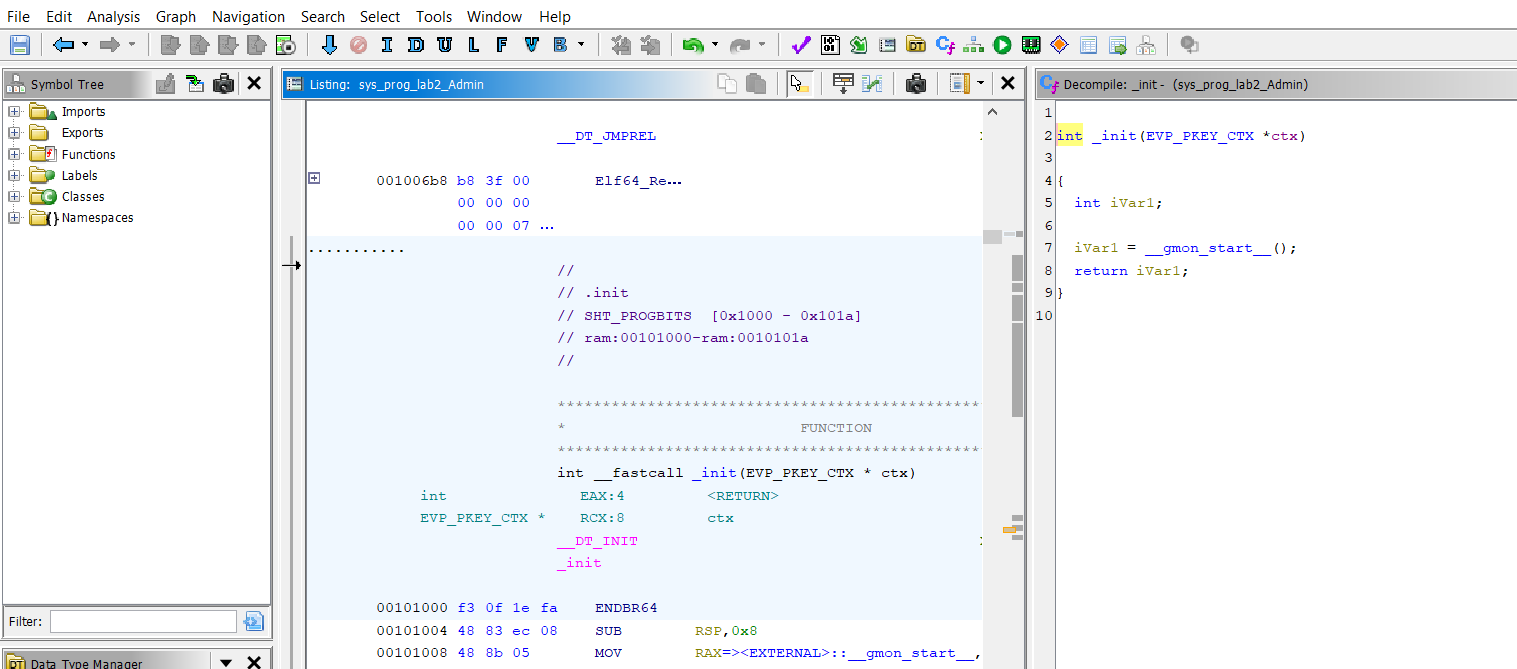


Рис. 5 – Виконання інжинірингу файлу «sys\_prog\_lab2»

Після чого необхідно знайти пароль в коді, для запустити програму “sys\_prog\_lab2\_your-nickname”, для цього було знайдено одну із небагатьох функції (getPass) та знайдено зчитування посимвольного паролю в умові if (рис. 6)

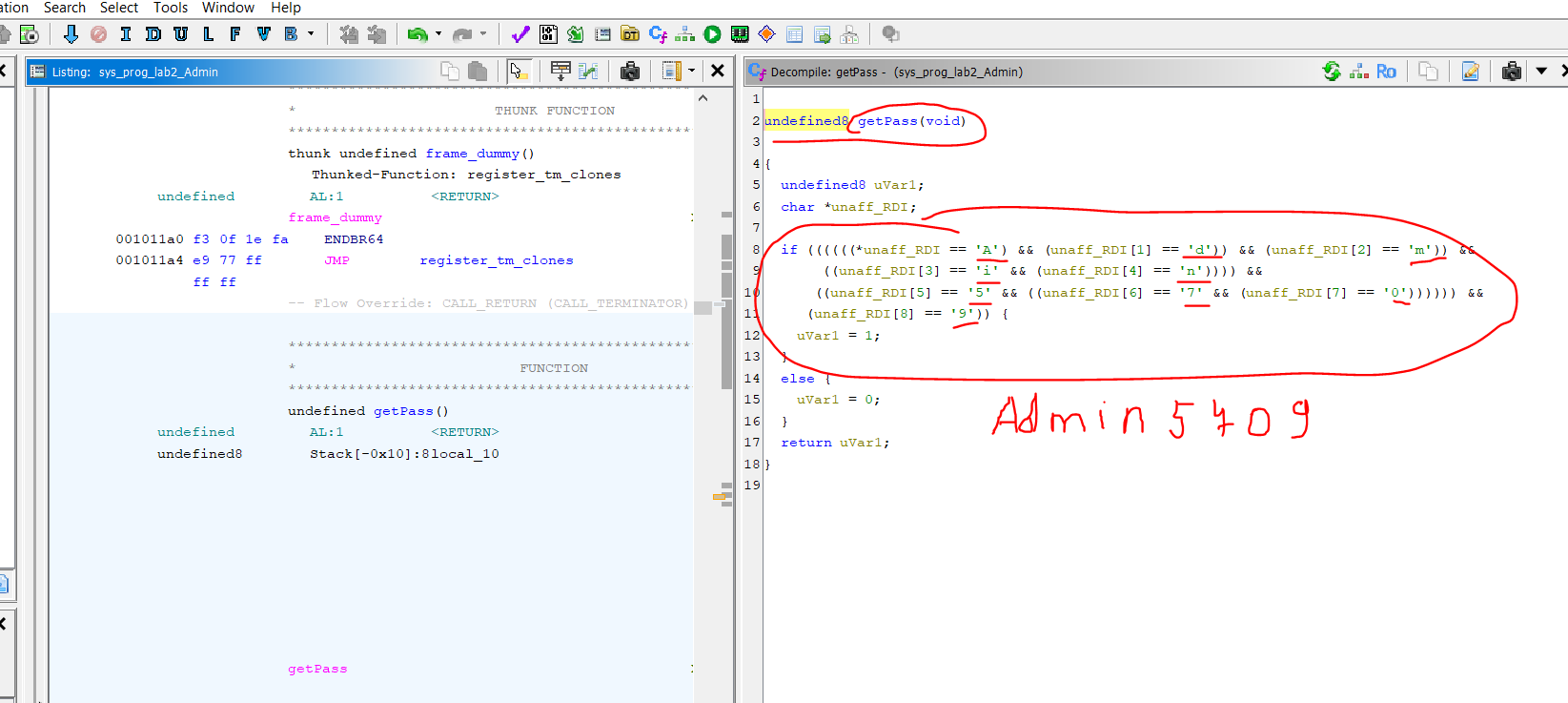


Рис. 6 - Знайдений пароль

Кінцевим етапом, запустимо програму «sys\_prog\_lab2», ввівши пароль (рис . 7)

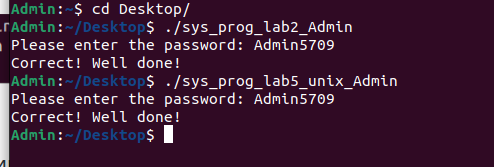


Рис. 7 – Виконання програми «sys\_prog\_lab2»

Висновки: У ході виконання лабораторної роботи, вивчила процес реверс інжинірингу програми з метою вивчення її поведінки.