Петров Д.М. КІТ-М120Б

Редагування файлу, що виконується

Мета

Дослідити особливості редагування файлу, що виконується.

Індивідуальне завдання:

Створити функцію, що виводить переданий рядок на екран. Реалізувати виклик даної функції безпосередньо void printMe (const char *) і через покажчик на функцію.

Визначте розмір кода виклику з урахуванням занесення аргументів в стек для обох випадків.

За допомогою hex редактора (напр. Hexedit) занулити виклики функцій, щоб їх виконання пропускалося.

Створити функцію, яка вводить пароль з клавіатури і порівнює його з "еталонним": bool isEqual(const char * expected).

Змінити асемблерний (машинний) код програми таким чином, щоб при введенні невірного пароля програма "думала", що пароль вірний і надавала доступ для подальшої роботи.

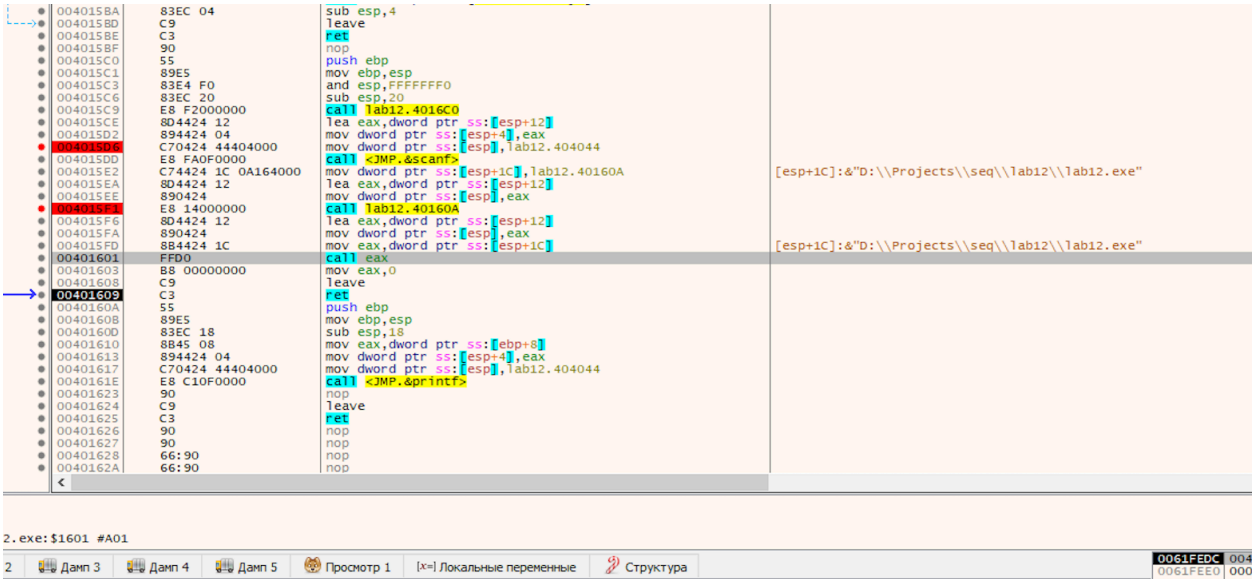
У звіті навести результати дослідження та кроки проведення змін файлу, що виконується.

Хід виконання:

Розробимо текст простої програми. Виділення статичного масиву символів та виклик функції scanf.

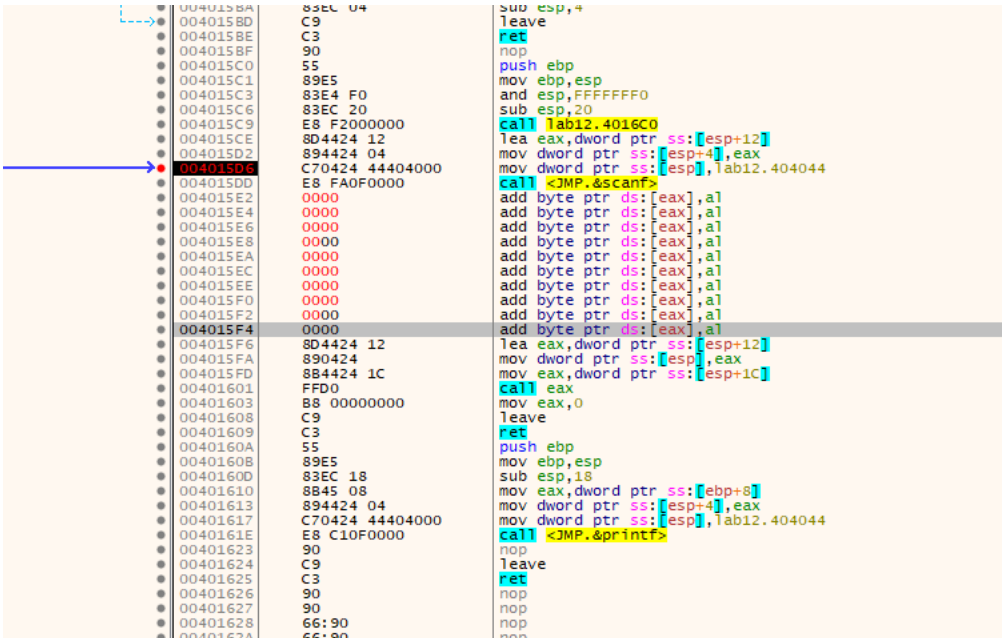
```
#include<stdio.h>

void printMe(const char * ptr);

int main() {

	char a[10];
	scanf("%s", a);
	void(*ptrPrint)(char*) = printMe;
	printMe (a);
	ptrPrint (a);
	return 0;
}


void printMe (const char * ptr) {
	printf("%s", ptr);
};
```

Розміри команд:
Явний виклик:
Усього – 20 байтів.
Неявний виклик:
Усього – 13 байтів.



Відкриємо файл у hex-editor та виконаємо пошук цих двох викликів

```
000009e0  00 00 c7 44 24 1c 0a 16  40 00 8d 44 24 12 89 04  ..ЗD$...@..D$.‰.
000009f0  24 e8 14 00 00 00 8d 44  24 12 89 04 24 8b 44 24  $и.....D$.‰.$‹D$
00000a00  1c ff d0 b8 00 00 00 00  c9 c3 55 89 e5 83 ec 18  .яРё....ЙГU‰eѓм.
00000a10  8b 45 08 89 44 24 04 c7  04 24 44 40 40 00 e8 c1  ‹E.‰D$.З.$D@@.иБ
```



Висновки:

Дослідили особливості редагування файлу, що виконується.