

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.

| | | | |
|----------|--------------------|--|---|
| 004015BA | 83EC 04 | sub esp,4 | |
| 004015BD | C9 | leave | |
| 004015BE | C3 | ret | |
| 004015BF | 90 | nop | |
| 004015C0 | 55 | push ebp | |
| 004015C1 | 89E5 | mov ebp,esp | |
| 004015C3 | 83E4 F0 | and esp,FFFFFFF0 | |
| 004015C6 | 83EC 20 | sub esp,20 | |
| 004015C9 | E8 F2000000 | call lab12.4016C0 | |
| 004015CE | 8D4424 12 | lea eax,dword ptr ss:[esp+12] | |
| 004015D2 | 894424 04 | mov dword ptr ss:[esp+4],eax | |
| 004015D6 | C70424 44404000 | mov dword ptr ss:[esp],lab12.404044 | |
| 004015DD | E8 FA0F0000 | call <JMP.&scanf> | |
| 004015E2 | C74424 1C 0A164000 | mov dword ptr ss:[esp+1C],lab12.40160A | [esp+1C]:&"D:\\Projects\\seq\\lab12\\lab12.exe" |
| 004015E4 | 8D4424 12 | lea eax,dword ptr ss:[esp+12] | |
| 004015E8 | 890424 | mov dword ptr ss:[esp],eax | |
| 004015F1 | E8 14000000 | call lab12.40160A | |
| 004015F6 | 8D4424 12 | lea eax,dword ptr ss:[esp+12] | |
| 004015FA | 890424 | mov dword ptr ss:[esp],eax | |
| 004015FD | 8B4424 1C | mov eax,dword ptr ss:[esp+1C] | [esp+1C]:&"D:\\Projects\\seq\\lab12\\lab12.exe" |
| 00401601 | FFD0 | call eax | |
| 00401603 | B8 00000000 | mov eax,0 | |
| 00401608 | C9 | leave | |
| 00401609 | C3 | ret | |
| 0040160A | 55 | push ebp | |
| 0040160B | 89E5 | mov ebp,esp | |
| 0040160D | 83EC 18 | sub esp,18 | |
| 00401610 | 8B45 08 | mov eax,dword ptr ss:[ebp+8] | |
| 00401613 | 894424 04 | mov dword ptr ss:[esp+4],eax | |
| 00401617 | C70424 44404000 | mov dword ptr ss:[esp],lab12.404044 | |
| 0040161E | E8 C10F0000 | call <JMP.&printf> | |
| 00401623 | 90 | nop | |
| 00401624 | C9 | leave | |
| 00401625 | C3 | ret | |
| 00401626 | 90 | nop | |
| 00401627 | 90 | nop | |
| 00401628 | 66:90 | nop | |
| 0040162A | 66:90 | nop | |

2.exe:\$1601 #A01

2 [Данп 3] [Данп 4] [Данп 5] [Просмотр 1] [x=] Локальные переменные [Структура] 0061FEDC 004 0061FEE0 000

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 ..3D$....@..D$.%.
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....ЙГУ%еѐм.
00000a10 8b 45 08 89 44 24 04 c7 04 24 44 40 40 00 e8 c1 <Е.%D$.З.$D@@.иБ

```

| | | | |
|----------|-----------------|-------------------------------------|--|
| 004015BA | 83EC 04 | sub esp,4 | |
| 004015BD | C9 | leave | |
| 004015BE | C3 | ret | |
| 004015BF | 90 | nop | |
| 004015C0 | 55 | push ebp | |
| 004015C1 | 89E5 | mov ebp,esp | |
| 004015C3 | 83E4 F0 | and esp,FFFFFFF0 | |
| 004015C6 | 83EC 20 | sub esp,20 | |
| 004015C9 | E8 F2000000 | call lab12.4016C0 | |
| 004015CE | 8D4424 12 | lea eax,dword ptr ss:[esp+12] | |
| 004015D2 | 894424 04 | mov dword ptr ss:[esp+4],eax | |
| 004015D6 | C70424 44404000 | mov dword ptr ss:[esp],lab12.404044 | |
| 004015DD | E8 FA0F0000 | call <JMP.&scanf> | |
| 004015E2 | 0000 | add byte ptr ds:[eax],al | |
| 004015E4 | 0000 | add byte ptr ds:[eax],al | |
| 004015E6 | 0000 | add byte ptr ds:[eax],al | |
| 004015E8 | 0000 | add byte ptr ds:[eax],al | |
| 004015EA | 0000 | add byte ptr ds:[eax],al | |
| 004015EC | 0000 | add byte ptr ds:[eax],al | |
| 004015EE | 0000 | add byte ptr ds:[eax],al | |
| 004015F0 | 0000 | add byte ptr ds:[eax],al | |
| 004015F2 | 0000 | add byte ptr ds:[eax],al | |
| 004015F4 | 0000 | add byte ptr ds:[eax],al | |
| 004015F6 | 8D4424 12 | lea eax,dword ptr ss:[esp+12] | |
| 004015FA | 890424 | mov dword ptr ss:[esp],eax | |
| 004015FD | 8B4424 1C | mov eax,dword ptr ss:[esp+1C] | |
| 00401601 | FFD0 | call eax | |
| 00401603 | B8 00000000 | mov eax,0 | |
| 00401608 | C9 | leave | |
| 00401609 | C3 | ret | |
| 0040160A | 55 | push ebp | |
| 0040160B | 89E5 | mov ebp,esp | |
| 0040160D | 83EC 18 | sub esp,18 | |
| 00401610 | 8B45 08 | mov eax,dword ptr ss:[ebp+8] | |
| 00401613 | 894424 04 | mov dword ptr ss:[esp+4],eax | |
| 00401617 | C70424 44404000 | mov dword ptr ss:[esp],lab12.404044 | |
| 0040161E | E8 C10F0000 | call <JMP.&printf> | |
| 00401623 | 90 | nop | |
| 00401624 | C9 | leave | |
| 00401625 | C3 | ret | |
| 00401626 | 90 | nop | |
| 00401627 | 90 | nop | |
| 00401628 | 66:90 | nop | |
| 0040162A | 66:90 | nop | |

Висновки:

Дослідили особливості редагування файлу, що виконується.