Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра Обчислювальна техніка та програмування

Звіт з лабораторной роботи з дисциплиі « Реверсне програмування »

Лабораторна робота 1

Виконав ст.гр. КІТ–36

Надірян Г.О.

Перевірив

Челак В.В.

Харків 2019

**Лабораторна робота 1**

**Тема**: «Реверсінг простих програм із запитом пароля»

##### Мета: Набути практичних навичок написання та застосування програм перевірки пароля і виправлення пароля в ехе-файлах в середовищі masm64.

##### Постановка задачі

1. Написати програму в середовищі masm64 відповідно до варіанта завдання. 2. Як запрошення на введення пароля вивести «зірочки» в кількості, яка дорівнює кількості букв прізвища автора програми і в якості пароля також використовувати прізвище автора програми.

3. У частині програми, яка відповідає за аналіз введеного пароля використовувати кілька власних процедур, які розташувати в різних місцях основної програми.

4. Вивести директорію знаходження програми, а також результати виконання програми через функцію MessageBox. Програму і результати привести в звіті. 5. Привести скріншоти послідовності пошуку пароля.

**Індивідуальне завдання**

Задана матрица 4 х 7. В первой строке матрицы определить сумму четных элементов, а в 3-й строке – нечетных. (Проверка пароля с помощью строковых команд). (ВАРИАНТ - 12)

include win64a.inc

.data

DATE1 STRUCT ; тип данных СТРУКТУРА с именем DATE1

elem1 dd ? ; имя первого поля структуры

elem2 dd ? ; имя второго поля структуры

elem3 dd ? ; имя третьего поля структуры

elem4 dd ? ; имя четвертого поля структуры

elem5 dd ? ; имя четвертого поля структуры

elem6 dd ? ; имя четвертого поля структуры

elem7 dd ? ; имя четвертого поля структуры

DATE1 ENDS

Password db "nadirian" ; проверка только первых пяти символов

len1 equ ($-Password)/type Password

Buf dq 8 ;

Err1 dq 0

Msg1 db "Пароль совпал",0

Msg2 db "Пароль не корректен",0

Title1 db "Проверка пароля",0

Title2 db "Тсс,пароль Надирян (на латинице в нижнем регистре)",0

stdout dq 0 ;

stdin dq 0 ;

cRead dq 0 ;

cWritten dq 0 ;

\_a dd 0;

\_b dd 0;

Msg db "\*\*\*\*\*\*\*\*",10,0 ;

.code

Pas1 proc

lea rsi,Password ; адрес первого элемента строки

lea rdi,Buf ; адрес второго элемента строки

mov rcx,len1

repe cmpsb ; побайтно проверяется len раз

jz m2 ;

inc Err1 ; счетчик несовпадений

m2:

ret

Pas1 endp

WinMain proc

sub rsp,28h;

mov rbp,rsp

invoke GetStdHandle,STD\_OUTPUT\_HANDLE

mov stdout,rax

invoke GetStdHandle,STD\_INPUT\_HANDLE

mov stdin,rax

invoke WriteConsole,stdout,ADDR Msg,sizeof Msg,ADDR cWritten,0

invoke ReadConsole,stdin,ADDR Buf,8,ADDR cRead,0

invoke Pas1

.if (Err1==0);

invoke MessageBox,0,addr Msg1,addr Title1,MB\_OK

.data

dir db 256 dup(0) ;переменная для хранения пути к текущей директории

align 8 ; выравнивание памяти по адресам, кратным 8 байтам

str1 DATE1 <2,2,2,2,1,1,1> ; структура с именем str1

str2 DATE1 <0,0,0,1,1,1,1> ; структура с именем str2

str3 DATE1 <2,2,2,1,1,1,0> ; структура с именем str2

str4 DATE1 <0,0,0,0,0,0,0> ; структура с именем str2

titl1 db "Вычисление..",0

buf1 dq 10 dup(0);

ifmt db "Задана матрица:",0dh,0ah,0ah,\

"2 2 2 2 1 1 1",0dh,0ah,\

"0 0 0 1 1 1 1",0dh,0ah,\

"2 2 2 1 1 1 0",0dh,0ah,\

"0 0 0 0 0 0 0",0dh,0ah,0ah,\

"Результат сложения четных элементов строки №1 массива =%d",0dh,0ah,\

"Результат сложения нечетных элементов строки №3 = %d",0ah,\

"Путь к файлу %s ",0

.code

xor edi,edi ; заполнение нулями

mov ebx,1 ; загрузка количества строк

lea rsi,str1 ; загрузка адреса первой строки структуры

m5: mov ecx,7 ; количество элементов в строке

m3: mov eax,dword ptr[rsi] ; загрузка элемента из строки структуры

test eax,1

je m1

jnz m2

m1: add edi,eax

mov \_a,edi ; сложение нечетных элементов строки структуры

m2: add rsi,4 ; подготовка адреса нового элемента

loop m3

dec ebx ; ebx := ebx 1

jz m9

;jz m4 ; если ebx = 0 (z = 1), то переход в заключение

jmp m5 ; переход на новый цикл

;m4:

m9:

xor edi,edi

xor ebx,ebx

xor rsi,rsi

xor ecx,ecx

xor eax,eax

mov ebx,1 ; загрузка количества строк

lea rsi,str3 ; загрузка адреса первой строки структуры

m15: mov ecx,7 ; количество элементов в строке

m13: mov eax,dword ptr[rsi] ; загрузка элемента из строки структуры

test eax,1

jnz m11

jz m12

m11: add edi,eax

mov \_b,edi ; сложение нечетных элементов строки структуры

m12: add rsi,4 ; подготовка адреса нового элемента

loop m13

dec ebx ; ebx := ebx 1

jz m4

m4:

invoke GetCurrentDirectory,255,addr dir; получение директории

invoke wsprintf,ADDR buf1,ADDR ifmt,\_a,\_b,addr dir

invoke MessageBox,0,addr buf1,addr titl1,MB\_OK

.else

invoke MessageBox,0,addr Msg2,addr Title2,MB\_ICONWARNING

.endif

invoke ExitProcess,0

WinMain endp

end

**Робота програми**

Запрошення на введення пароля

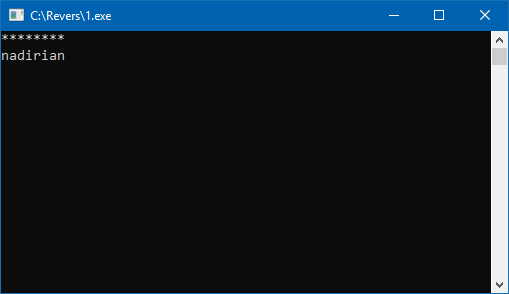


Рисунок 1 - Запрошення на введення пароля вивести

Позитивний сценарій вводимо вірний пароль і натискаємо ок (рис.1.2. та рис.1.3.)

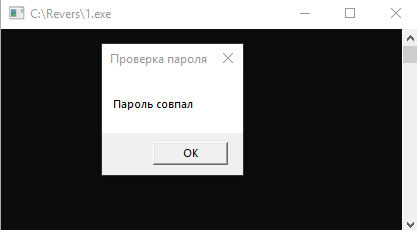


Рисунок 2 - Вводимо вірний пароль

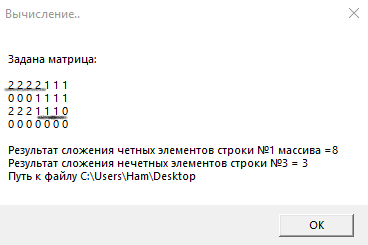


Рисунок 3 - Після натискання “Ok”

Негативний сценарій вводимо невірний пароль

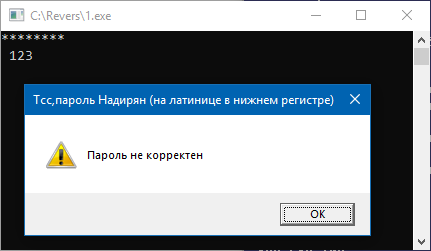


Рисунок 4 - Вводимо невірний пароль

**Реверсінг**

Аналізуючи вміст полів команд порівняння(рис..2.1.). У багатьох випадках порівняння відбувається за допомогою команди cmp. Наступним рядком після команди порівняння cmp розташована команда *jne 1.7ff718c21142.* Яка в разі нерівності операндів (за ознакою ZF) перейде наадресу *7ff718c21142.* А якщо по команді jnz вміст комірки пам'яті з адресою *7FF718с21000* і нуля співпадуть, то можна зробити припущення, що паролі збіглися. Тому треба виправити код операції так, щоб після введення довільного пароля, результат був правильним.

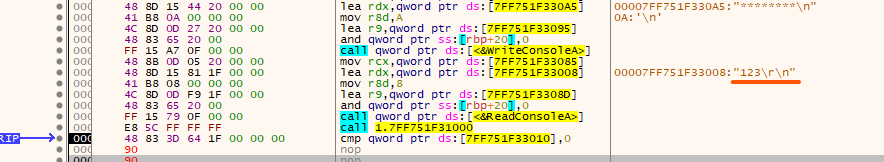


Рисунок 5 - Аналіз вміст полів команд порівняння

Щоб виключити команду переходячи за умовою необхідно вставити команди nop. Для цього підводимо курсор до рядка з командою jne pas4-64-2.7FF78FE21148, двічі натискаємо ліву клавішу мишки, ставимо позначку у віконці Заповнити командами NOP і вводимо NOP (рис.2)

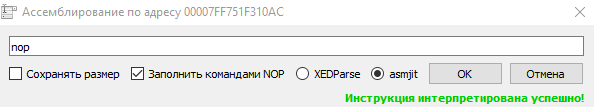


Рисунок 6 - вставка команди nop

**Внесення змін**

Вибираємо Файл / Виправити файл (рис.3.1.). У новому вікні вибрати пункт Виправити файл. Потім - нове ім'я і розширення ехе(рис.3.2.)

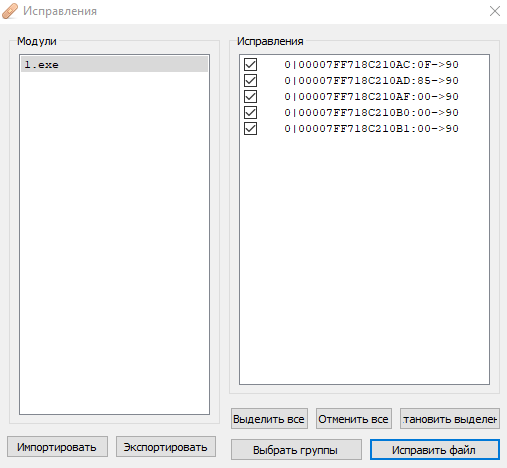


Рисунок 7 - Внесення змін

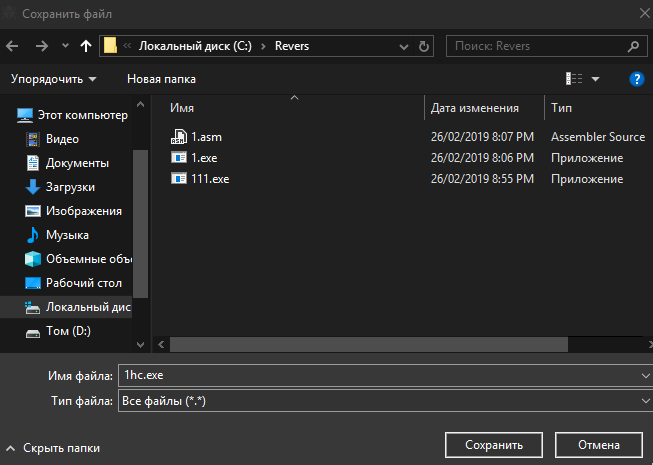


Рисунок 8 - Збереження файлу

Запуск програми вводимо невірний пароль (рис.4.1. та рис.4.2.)

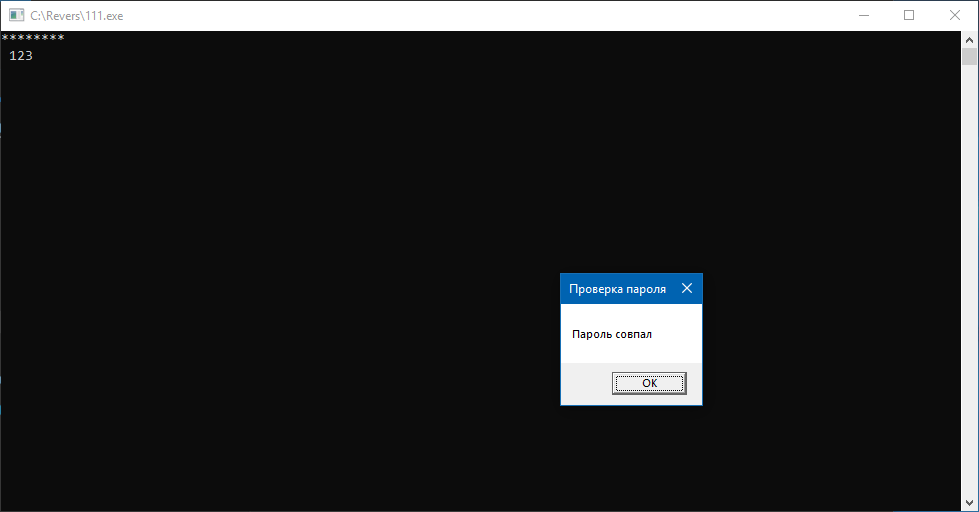


Рисунок 9 - Запуск програми вводимо невірний пароль

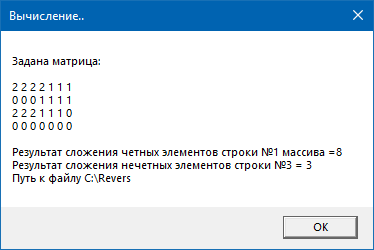


Рисунок 10 - Після натискання “Ok”

**Висновок**

Написали програму в середовищі masm64 відповідно до варіанта завдання.

У частині програми, яка відповідає за аналіз введеного пароля використовували кілька власних процедур, які розташувати в різних місцях основної програми. Вивели директорію знаходження програми, а також результати виконання програми через функцію MessageBox. Програму і результати привели в звіті. Виправили пароль в ехе-файлах в середовищі masm64.