MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL TECHNICAL UNIVERSITY

"KHARKIV POLYTECHNICAL INSTITUTE"

Department of Computer Engineering and Programming

«Software Means of Information Protection »

*Laboratory work report No 5*

*Topic: «* **Overlapping instructions** *»*

Student:

Group. KH 919 I.E

Ayoub EL-HADDADI

Verified by:

Lecturer Viktor CHELAK

Kharkiv – 2022

***Purpose of work***:

To acquire practical skills in writing and applying password-checking and password-correction programs in ex-files in masm64 environment with data placement in code pages and code overlaps.

***Individual task:***

Use the AVX commands to execute an equation where variable a takes five values and is given by an array. The remaining numbers are also specified in the array {b, c, d, and e}. Print result via MessageBoxIndirect. Numbers are specified in arrays. Apply as many receptions as possible with code overlap.

Variant 8:

**Algorithm of the program**

First step of the program is a password checker, using a created password verification procedure, we simply compare two strings (input, with the real password) and increase a variable in case of error.

Second, is we check AVX command support issued with a call of separated executable file, “AVX.exe” and its source code can be found in same folder “AVX.asm”.

Then, we move to part of working with the equation. We’ve initialized an array of “a” (array A = {a1, a2, a3, a4, a5} with 5 random values, and constants “b, c, d and e”, we move each constant to a register “xmm”, and calculate and store it in xmm5 as a constant.

Next step is we move into a loop, and calculate result of equation for every “a” value in array A, for such reasons we use AVX command, and we are going to need:

VSQRTSD - Compute Square Root of Scalar Double-Precision Floating-Point Value

VMULSD - Multiply Scalar Double-Precision Floating-Point Value

VCVTTSD2SI - Convert with Truncation Scalar Double-Precision Floating-Point Value to Signed Integer

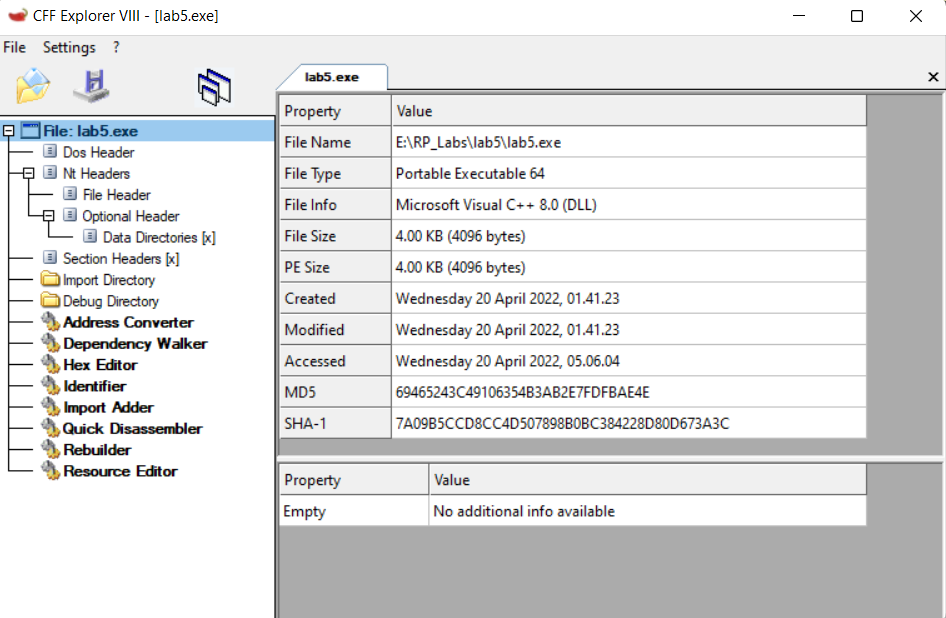
VDIVSD - Divide Scalar Double-Precision Floating-Point Value

VSUBSD - Subtract Scalar Double-Precision Floating-Point Value

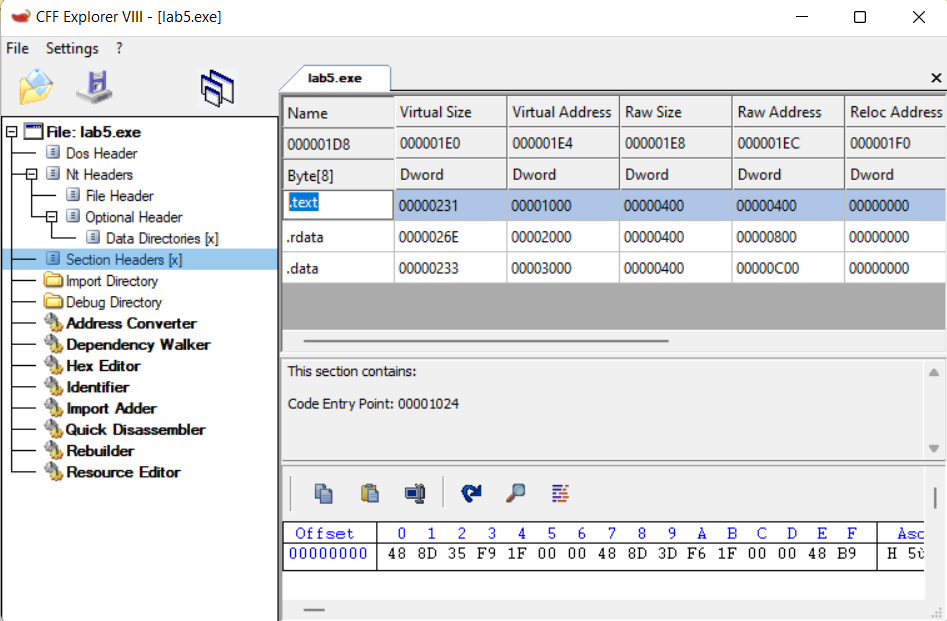
We fill an empty array with results and output result via MessageBoxIndirect

Injection in an executable file

Rename the code section to a non-system name, for that we use CFF\_Explorer program.

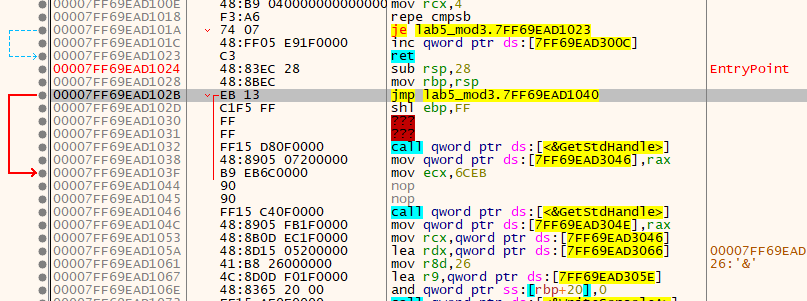


In left side we can see “Section Headers” in which all section can be found and created

****

Double click on section name and we can rename it as required. Next step is to save the file as new copy or in the same executable file.

Next we use x64dbg to make code overlap, we edit a line with a mov instruction to ecx with a size of the jump and a jump instruction into the middle of this command, to overlap the code into message box of correct password.



And the same think for second overlap to skip calculation of equation into message box and output of initialized array of results.

**Source Code**

Full source code of this lab you can find it in:

[**https://github.com/Elh-Ayoub/RP\_Labs/tree/main/lab5**](https://github.com/Elh-Ayoub/RP_Labs/tree/main/lab5)

**Results of the program:**

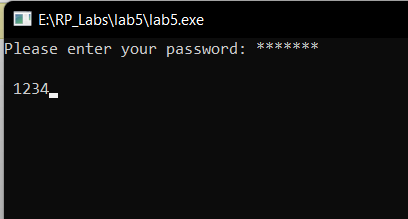


Figure 1 – Password request

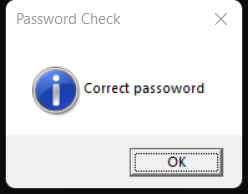


Figure 2 – Correct password message box



Figure 3 – Invalid password message box

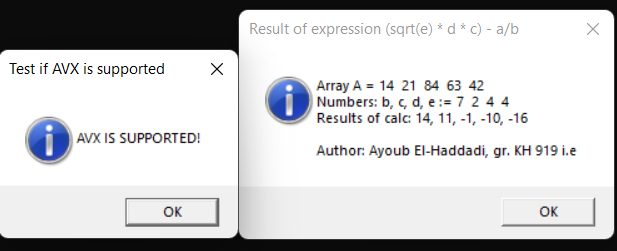


Figure 4 – AVX.exe and message box with results

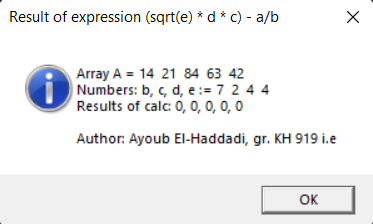
****

Figure 5 – Modified lab5.exe

**Conclusions:**

As a result of laboratory work we gained a practical skills in writing and applying password-checking and password-correction programs in ex-files in masm64 environment with data placement in code pages and code overlaps.

**You can also find this report in:**

<https://github.com/Elh-Ayoub/RP_Labs/tree/main/Docs>