|  |  |  |
| --- | --- | --- |
| Week | Reverse Engineering Malware | Duration |
| 12 | OLLYDBG Practical | 120 mins |

Marks allocation: 10/100 for CA practical submission

**Lesson Objectives**

The objective of this practical is to familiarise the students of how to use OllyDBG to reverse-engineer a PE.

# Lab 01 [120mins]

In this lab, you will try to reverse engineer the file: Q1.exe.

You can download the file <https://goo.gl/TnLhPj>

**Instructions**

Run the program and note the message box that the program displays. It seems that the program’s evaluation period has expired.



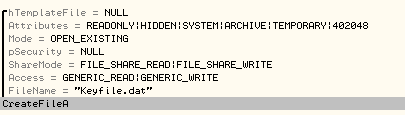
You need to reverse-engineer the program so that you can bypass the evaluation period check.

**Question 1**

What does the function located at address 0x401073 perform? The function is to create file (read an existing file or create a new file).



How many parameters do the function accepts? 7



**Question 2**

What is the return value when this function finishes executing? It returns an Handle to the specified resource.



What is the desired value? The file is existing.



**Question 3**

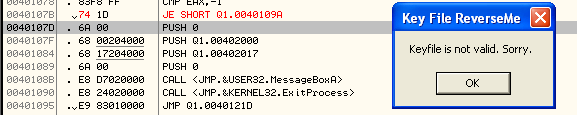
When will the jump taken at address 0x40107B?

If the file keyfile.dat is existing then the jump is taken. Jump taken if eax = -1, JNZ (Jump when the zero flag is not set)



Make the necessary changes for the jump to take place and run the program.

Modify the JNZ to JE or NOP.



You should see the following screen.



**Question 4**

What does the function located at address 0x4010A9 perform?



The function is to read file keyfile.dat.

**Question 5**

When is the jump located at 0x4010B0 taken? When the value of eax is 0. When the test result is 0 then the zero flag is set (ZF=1) and the jump will be taken.



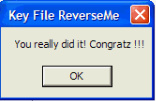
Make the necessary changes for the jump to take place.

Modify the JNZ to JE or NOP.

**Question 6**

Make all necessary changes so that you are able to see the following message box.

Make all conditions to NOP.



**Question 7**

Patch the file so that you can always display the “You really did it!” box every time you run the PE.

