|  |  |  |
| --- | --- | --- |
| Week | Reverse Engineering Malware | Duration |
| 2 | Introduction to IDA Pro and VS 2019 | 120 mins |

Marks allocation: 8/100 for CA practical submission

**Lesson Objectives**

1. Use IDA Pro to recognize and analyse code constructs to understand overall functionality of Assembly Language program
2. Execute assembly code in Visual Studio 2019.

Download the files from MeL.

# Lab 01 [10 mins]

Install IDA Pro 5 (idafree50.exe).

# Lab 02 [60 mins]

Analyze the file *REMWeek2Lab.exe*.

(Open IDA Pro – click new disassembly – select the PE file - *REMWeek2Lab.exe*.)

Check on Analysis Option and leave the other options as default.

**Question 1**

What is the major code construct found in the only subroutine called by **main**?

(Hint: In the Text View go to the main function and right click to select graph view)

It is an if statement that prints a message depending on the outcome of the “InternetGetConnectedState” function. If the function returns 0, it will print a message stating there is no internet, otherwise it will print a message indicating the computer has an internet connection

**Question 2**

What is the subroutine located at 0x40105F? printf()

**Question 3**

What is the purpose of this program?

Check for internet connection and print out a message to indicate if there is any internet connection.

**Question 4**

Execute *REMWeek2Lab.exe with and without internet connection. What is the output*?

“Error 1.1: No Internet”

# Lab 03 [50 mins] (Self-Exploration)

1. Unzip Project32\_VS2019. (Make Sure C++ is installed in your Visual Studio 2019 Community Edition)
2. Download the required libraries from <http://asmirvine.com/gettingStartedVS2019/Irvine.zip>
3. Unzip the libraries in c:/Irvine folder (Make sure the C:/Irvine folder contains no subfolders inside)
4. Click on the solution file (.sln) to open up in Visual Studio 2019.
5. Refer to the instructions to debug the assembly code and checking the values of the registers:

<http://asmirvine.com/gettingStartedVS2019/index.htm>

1. Note: Students who have Visual Studio 2017 community edition need to download the project from: <http://asmirvine.com/gettingStartedVS2017/Project32_VS2017.zip> and refer to the instructions to debug the assembly code and checking the values of the registers:

<http://asmirvine.com/gettingStartedVS2017/index.htm>