|  |  |  |
| --- | --- | --- |
| Week | Reverse Engineering Malware | Duration |
| 7 | IDA Pro Practical | 60 mins |

Marks allocation: 10/100 for CA tutorial submission

**Lesson Objectives**

Use IDA Pro to recognize and analyse code constructs to understand overall functionality of Assembly Language program.

Lab files can be found on desktop folder (Labs) on the Windows XP Virtual Machine.

# Lab 01 [60 mins]

Analyze the malware found in the file *Lab06-02.exe*.

**Question 1**

What operation does the first subroutine called by main perform?

Main called subroutine sub\_401000 to check if there is internet

**Question 2**

What is the subroutine located at 0x40117F?

Printf subroutine is located in 0x40117F

**Question 3**

What does the second subroutine called by **main** do?

It is trying to connect to a website called [http://www.practicalmalwareanalysis.com/cc.htm](http://www.practicalmalwareanalysis.com/cc.htm&#8221)

**Question 4**

What type of code construct is used in this subroutine?

This subroutine use an array to store information read from an html file to try and retrieve a command by looking for command in the html file which start with “<!–“.

**Question 5**

Are there any network-based indicators for this program?

Yes, this is 2 network-based, there Is one use to attempt connection with the website and one use for user-agent it creates to connect to the URL “Internet Explorer 7.5/pma”.

**Question 6**

What is the purpose of this malware?

This malware first check if there is internet connection, if do not have, it will close. Else it will try to access the website and look for the comment in the HTML file and print out the comment, then sleep for 1 minute then close the malware.