|  |  |  |
| --- | --- | --- |
| Week | Reverse Engineering Malware | Duration |
| 11 | 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]

In this lab, we’ll analyze the malware found in the file *Lab06-04.exe*.

***Questions***

1. What is the difference between the calls made from the main method in

Labs 6-3 and 6-4?

In Labs 6-3, the printf is at 0x401271 and executeCommand is at 0x401130 but In Labs 6-4, the printf is at 0x4012B5 and executeCommand is at 0x401150.

2. What new code construct has been added to main?

A for loop is added to main.

3. What is the difference between this lab’s parse HTML function and those of the previous labs?

The difference is that in this lab a sprint is called at 0x401040, which add a extra argument to the User-Agent

4. How long will this program run? (Assume that it is connected to the Internet.)

It will run for 1440 minutes

5. Are there any new network-based indicators for this malware?

Yes, a new User Agent is used. It take Internet Explorer 7.5/pma[0-1439]

6. What is the purpose of this malware?

This malware first will check if there is internet connection. If there is no connection, close the program. Or else, it will use a user-agent to attempt to get the command in the website comment (which start with <!--) than create a directory, copy itself to that directory than delete itself from the old location and add a registry key to user system or sleep for 100 second, this programme will run for 24 hours before it terminated. Or else it will close the program