PROJ 11: Using OllyDbg to Analyze Lab09-01.exe

Prof. Alberto LaCava

CY -640

MALWARE ANALYSIS & DEFENSE

Nikhil Patel

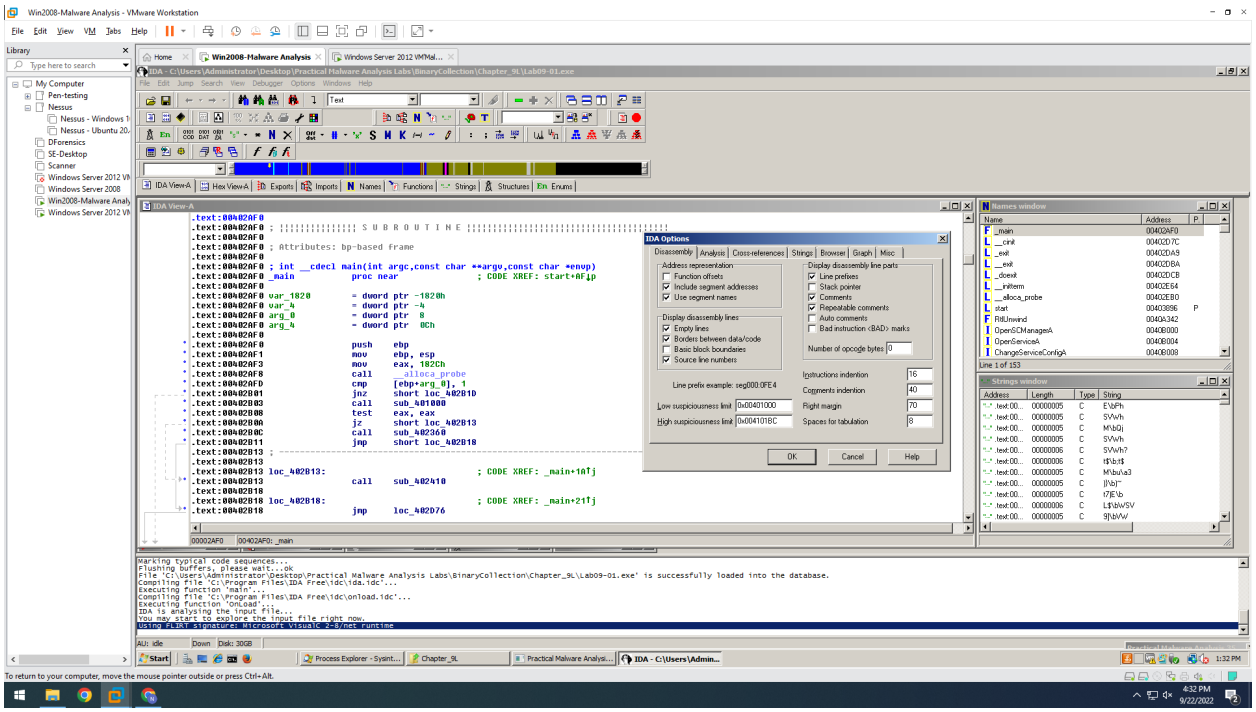
11/01/2022

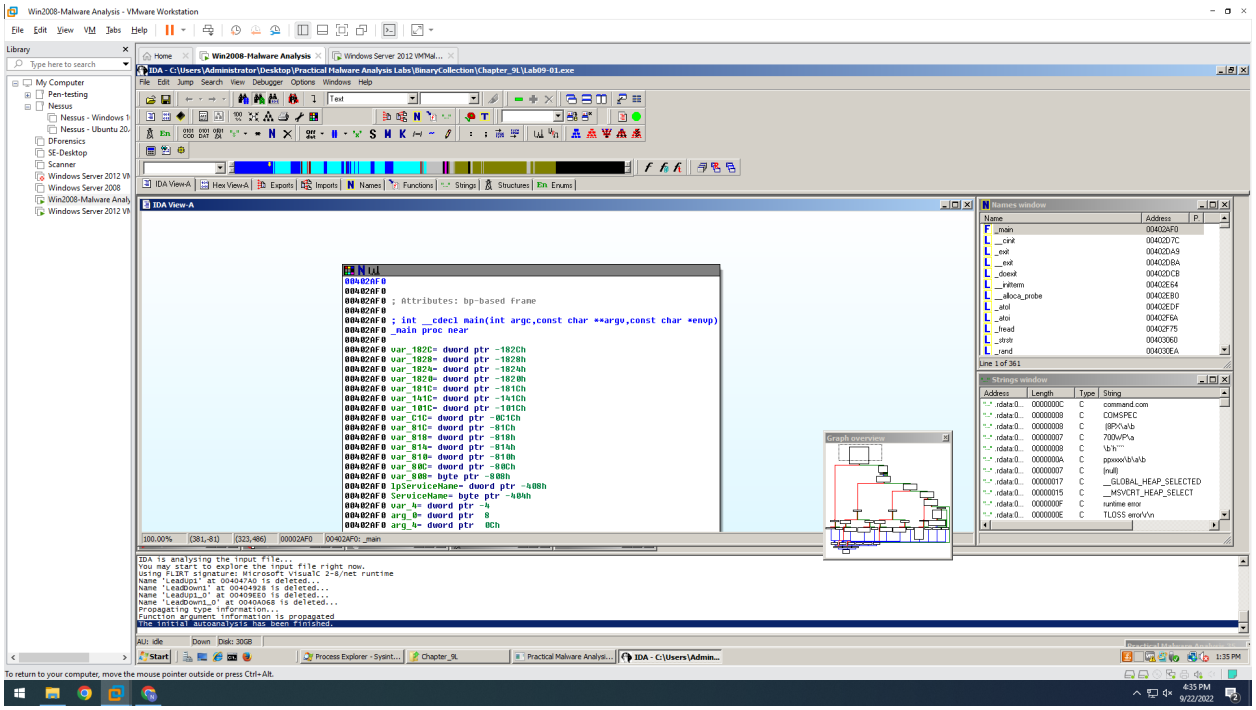
Introduction: In this lab, we will analyze the malware with IDA Pro (Lab 09-01.exe) and also demonstrate the use of OllDbg.

Procedure :

Finding the Main Entry Point

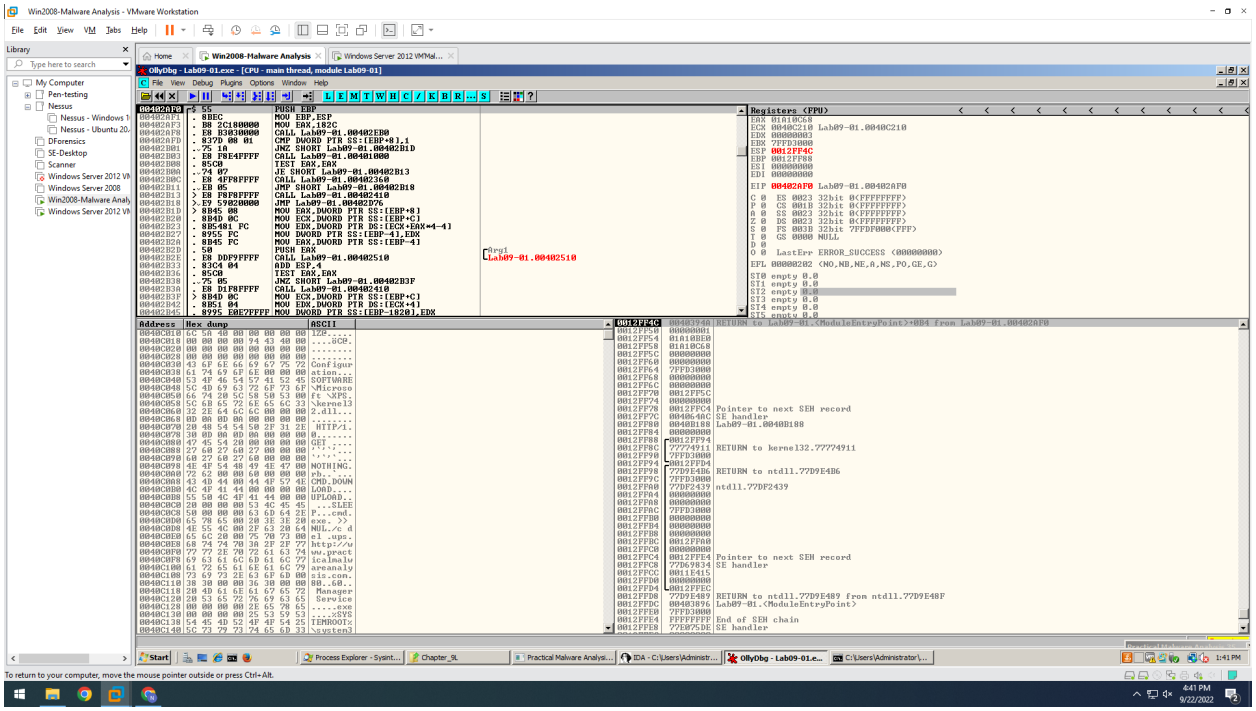
- Open the Lab09-01.exe file in IDA Pro and go to option > general and check Line Prefixed and hit OK.
- Now click on windows and then Reset Desktop.



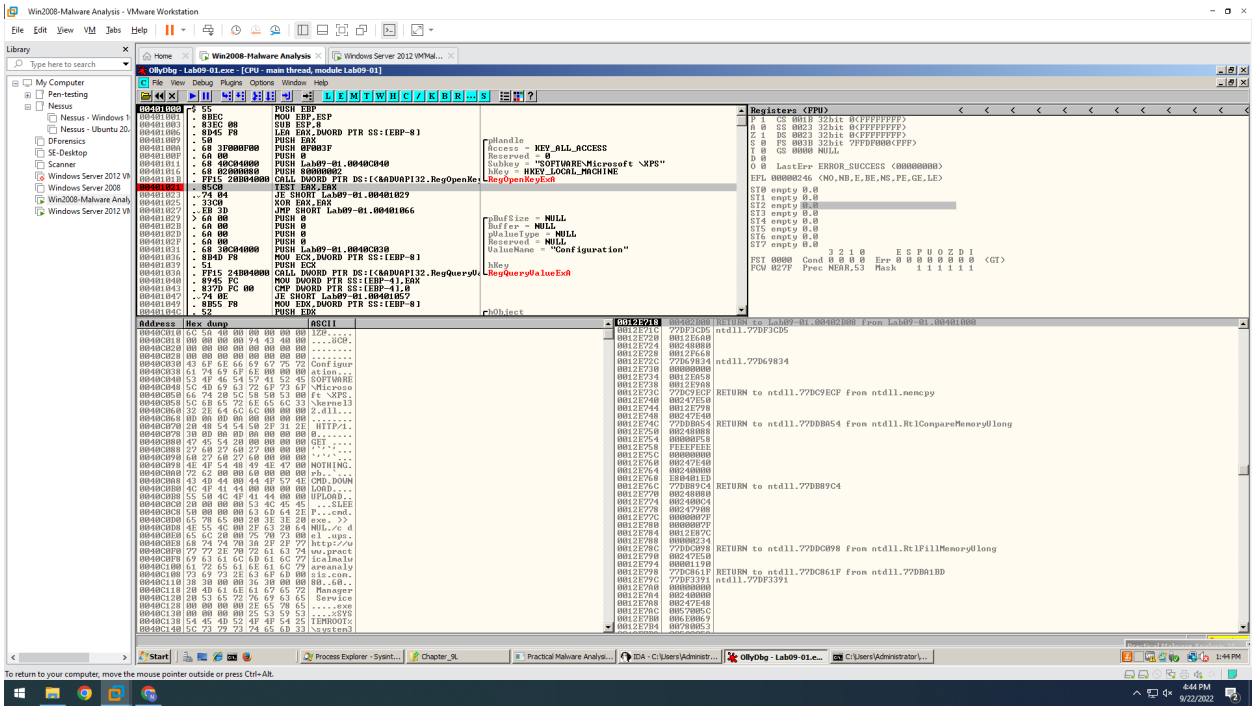


Using OllyDbg to Walk Through Quickly

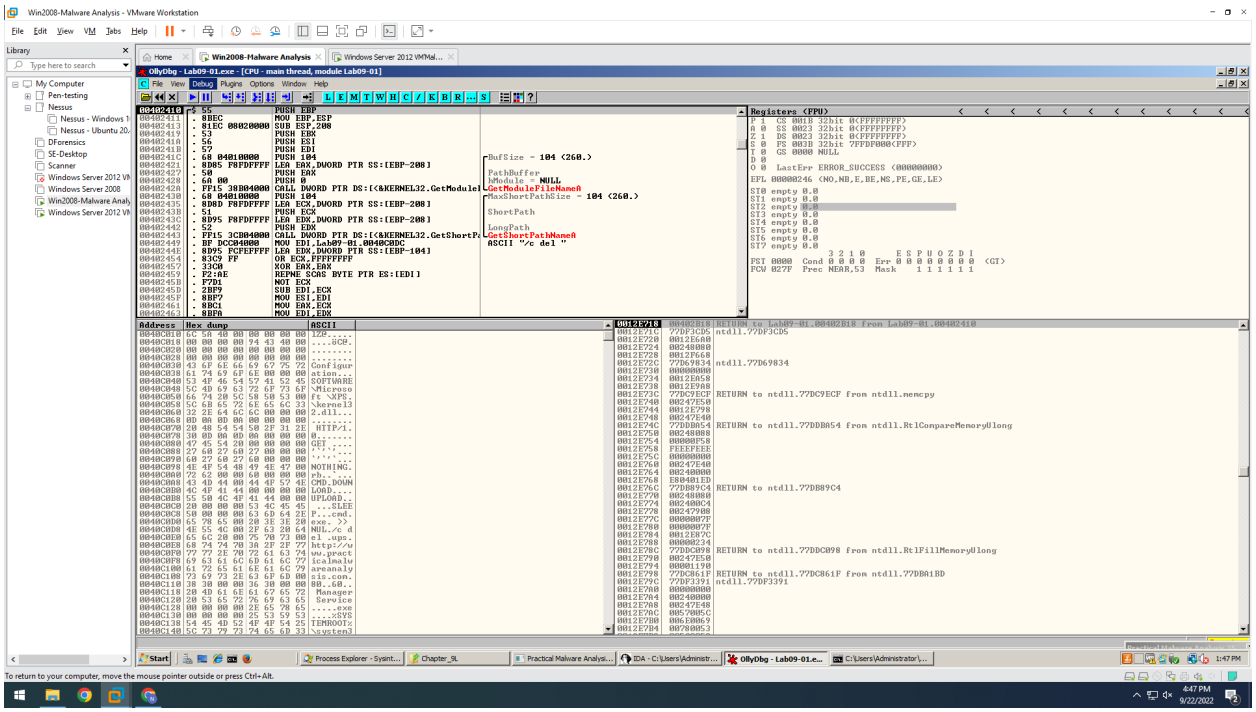
- Open Lab09-01.exe in OllyDbg.



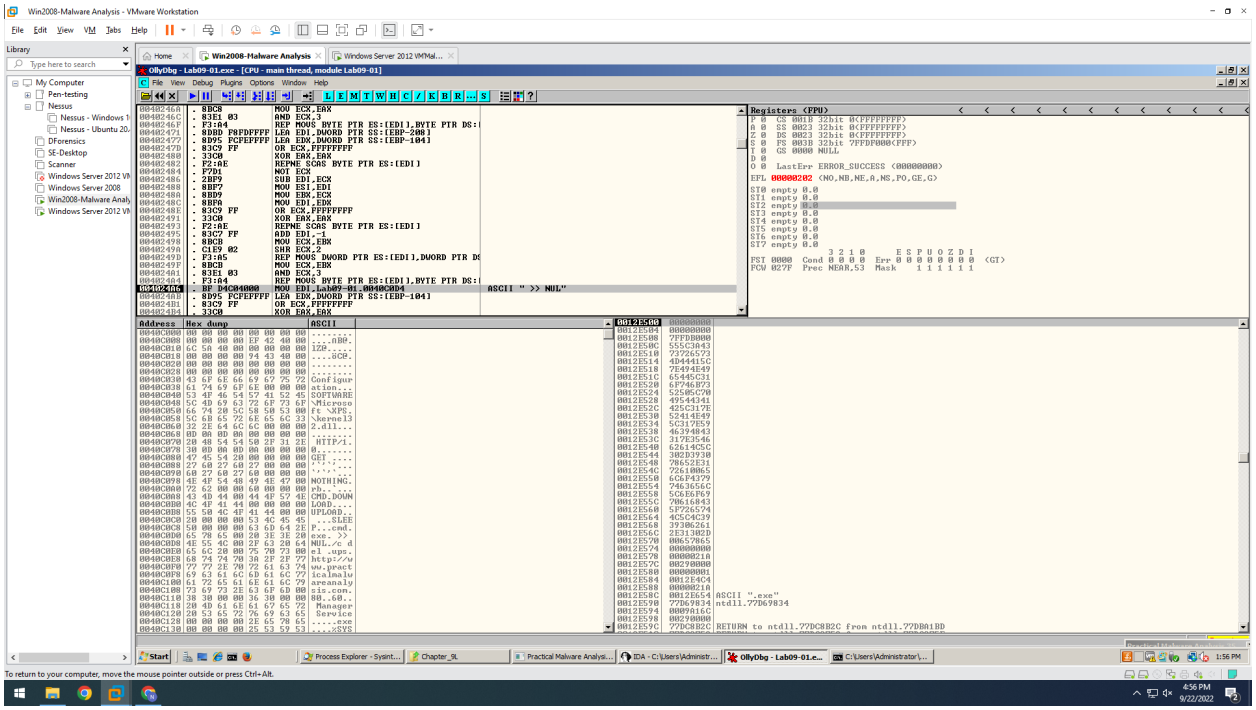
- Now Press F8 40 times to stop at 0x403999 on the right side of the screen you will see Arg 3,2, and 1.



- Now Press F7 5 times to load a parameter and call main from 0x403925.
- Now Press F7 20 times to call a short subroutine 0x402AFD.



- Now Press F7 3 times to pass the test and jump to 0x00401000.
- Left click on line starting with 0x401021 and press F2 to put a breakpoint, it will turn red.
- Go to 0x401000 left click on it and press F9 to run to the breakpoint.



Conclusion: To wrap off the lab, we learned how to use IDA Pro to study the malware in the Lab09-01.exe file, as well as a quick walkthrough using OllDbg.