# 8th Laboratory: Modify execution

Rodrigo Castillo

4 de octubre de 2020

## 1. Q: Read section "Debugging.ªnd identify the difference between a "disassembler.ªnd a "debugger", and between a "source-level debugger.ªnd an .ªssembly-level debugger".R:

- The main difference between a disassembler an a debugger is that a disassambler cant run instructions, it only print them, a debugger run instructions step by step , but not necesary print them
- a source-level debugger is a debugger that is made for debugging code, so for example, visual studio code has a debugger, an asembly level debugger is made for undertanding binaries, so it run machine instructions instead of code instructions

## 2. Debugging an application in user mode implies that the debugger application (WinDbg or OllyDbg) is running on the same system as the code being debugged. Explain how kernel debugging is performed?

## 3. Q: Read the section "Pausing Execution with Breakpoints.ªnd explain the differences between "Software Execution Breakpoints", "Hardware Execution Breakpoints.ªnd Çonditional Breakpoints"through the following table.

## 4. Table

**Software execution Breakpoints:**

1. Prupose of breakpoint:
2. Number of supported breakpoints:
3. How it works:
4. Drawbacks:

**Hardware execution Breakpoints**

1. Prupose of breakpoint:
2. Number of supported breakpoints:
3. How it works:
4. Drawbacks:

**Conditional Breakpoints:**

1. Prupose of breakpoint:
2. Number of supported breakpoints:
3. How it works:
4. Drawbacks:

5. Q: Read the section .Exceptions.and explain the difference between a first and second chance exception.

6. Q: Explain the differences between , an exception induced by a breakpoint, , an exception from a single-stepping and , a memory-access violation exception.

7. Q: Download OllyDBG from http://www.ollydbg.de/odbg110.zip and PowerISO from http://nourinfo.com/tools/Power%20ISO%20 Then, crack PowerISO to achieve to use the application without a valid registration code"

8. R: Put here a screenshot of PowerISO displaying the message: "Thanks for your registration"

9. Q: Try to open netcat using the arguments -l -p 443

10. R: Put here the full screenshot that show "ncrunning from the debugger and receiving messages by the port 443 sent from another console that has a telnet app started.

11. Q: From the previous questions. The address of netcat's System Startup breakpoint is at 7C91120F. The address of netcat's Entrypoint is at 00401160. Explain how may I control where the application being opened by Ollydbg is PAUSED?

12. Q: Read the section "The OllyDbg Interface.and explain what is contained in each of the four windows (Disasssembler window, Registers window, Stack window, Memory dump window) that are opened when OllyDBG starts an application.

13. Q: Read the section "(RAM) Memory Map.and explain in your own words the concept of rebased.and the issues that an .absolute address"brings.

14. Q: Read the section .Execute code.and explain how stepping-over works.

15. Q: Read the section "Breakpoints.and explain when would it be useful to employ a Çonditional breakpoint"(Fig 9-8).

16. Q: Read section "Loading DLLs.and try uploading