

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 and a debugger is that a disassembler can't run instructions, it only prints them, a debugger runs instructions step by step, but not necessarily prints them
 - a source-level debugger is a debugger that is made for debugging code, so for example, Visual Studio Code has a debugger, an assembly-level debugger is made for understanding binaries, so it runs 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 "Conditional Breakpoints" through the following table.**
4. **Table**

Software execution Breakpoints:

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

Hardware execution Breakpoints

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

Conditional Breakpoints:

1. Purpose 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 `EXCEPTION_BREAKPOINT`, an exception induced by a breakpoint, `EXCEPTION_SINGLE_STEP`, an exception from a single-stepping and `EXCEPTION_ACCESS_VIOLATION`, 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](http://nourinfo.com/tools/Power%20ISO%20) Then, crack PowerISO to achieve to use the application without a valid registration code”