Offensive Software Exploitation

Summer 2020

Ali Hadi

@binaryz0ne

Debugging…

Part #3

Debugger

- A computer program that lets you run your program, line by line and examine the values of variables or look at values passed into functions and let you figure out why it isn't running the way you expected it to.

Why use Debuggers

- Debuggers offer sophisticated functions such as:
  - Running a program step by step
  - Pausing the program to examine a current state
  - Tracking the values of variables, CPU registers, memory locations, etc and even change them at runtime
  - Attach to a running process
  - View the process's Memory map
  - Disassemble program instructions

Common Debuggers

- GNU Debugger (GDB)
- Microsoft Windows Debugger (Windbg)
- OllyDbg
- Immunity Debugger
  - Based on Ollydbg
- Microsoft Visual Studio Debugger
- Interactive DisAssembler (IDA Pro)

Disassemblers v. Debuggers

- A disassembler like IDA Pro shows the state of the program just before execution begins

- Debuggers show
  - Every memory location
  - Register
  - Argument to every function at any point during processing
    - And let you change them

Source-Level v. Assembly-Level Debuggers

- Source-level debugger
  - Usually built into development platform
  - Can set breakpoints (which stop at lines of code)
  - Can step through program one line at a time
  - Usually used by developers
- Assembly-level debuggers (low-level)
  - Operate on assembly code rather than source code
  - Breakpoints are set at instructions
  - Usually used by exploit developers and malware analysts

Two Ways for Debugging

- Start the program from within the debugger
- Attach the debugger to a running program

Using a Debugger

Demo

Q&A + DIY

- Can we modify executables using a debugger?
- Write an example showing howto modify a Windows EXE file using a debugger.
  - For example bypass a whole check routine or set of instructions!!!

References

- Sam Bowne, Malware Analysis Course Slides, http://samsclass.info/126/126_F13.shtml
- Practical Malware Analysis by Andrew Honig and Michael Sikorski, No Starch Press
- A Bug Hunter's Diary by Tobias Klein, No Starch Press