CS356: More Reverse Engineering

W. Michael Petullo

University of Wisconsin–La Crosse

As of December 1, 2021

More Reverse Engineering: Exercise

Complete Aquinas reveng1 in C.

1. Run `readelf -SW hellobye` and `readelf --relocs hellobye`
2. Run `gdb hellobye`
   - `break main` and `run`
   - `si` twice (Confirm `rip` in .plt)
   - `disassemble`
   - `print $rip+M+0xNNNN` (Confirm `jmp` target in .got.plt)[1]
   - `x/x $rip+M+0xNNNN` (Back where we started: push slot; jump to start of `.plt`)
   - Then: `push 0x2fe2(%rip)`; `jmp *0x2fe4(%rip)`
   - At `*0x2fe4(%rip)` we find ourselves in `_dl_runtime_resolve_xsavec`
   - `break hellobye.c:5` and `continue`
   - `si` twice (Confirm `rip` in .plt)
   - `disassemble`
   - `print $rip+M+0xNNNN` (Confirm in .got.plt)

[1] +M (inst. width) because inst. not fetched/RIP not advanced

More Reverse Engineering: Assignments

Graded Homework Aquinas: reveng2, reveng3, and reveng4

`https://www.flyn.org/courses/cs356/schedule`