Intro to Reverse Engineering

Day 1

Rowan Hart

September 11, 2020

General Announcements & Introduction

- CSAW is this weekend! Everyone should play!
- Sign up for the bootcamp CTF at https://play.ctf.b01lers.com
- I will answer questions from Twitch, Youtube, and Discord.
- Docker container instructions are at https://ctf.b01lers.com/docker.html
- Source code is at https://github.com/b01lers/bootcamp-2020-rev
- TODAY WILL BE SHORTER!

Selection Recap

Lets recap selection using a new tool: Godbolt CE!
https://godbolt.org/z/E65Mrn

Reversing Tools

SREs:

- Ghidra
- Radare2 (CLI + Radare2 Cutter GUI)
- Binary Ninja (Paid)
- IDA (Free version, Home Edition)

Other Tools:

- GDB + Gef (or Pwndbg, Peda)
- Angr
- Z3
- Godbolt CE

Iteration

We will examine iteration, or looping:
https://godbolt.org/z/zznG98

Structures

Do you like OOP? We will look at some C++ / C structures and dive in to some of the more advanced but excellent features of Ghidra.
Once again, easier to show with a demo.
Simple structures:
https://godbolt.org/z/xWjWx9
More complex structures:
https://godbolt.org/z/ej8a8n

Obfuscation

Obfuscation techniques include:

- Hidden calls
- Encrypted strings
- Packed binaries
- Stripped binaries
- Simple optimization

Some Demos

Finally, lets check out some demos of real challenges and how to approach solving them.

Advanced RE Tools + Techniques

We'll talk a small amount about:

- GDB Scripting
- Z3 Solver
- Angr