A gentle introduction to reverse engineering

Alexander Bergenholtz

November 3, 2020

Examine the file

- Run the program! (Safely.)
- Examine output.
- Look for strings
- Imported functions, exported functions.
- Link type.
- `file`, `strings`, `readelf`, `objdump`,
- Pay close attention to details.
- Elf format / How does the elf header work.

Tools (S+ tier general purpose tools, non-exhaustive)

- [Ghidra]
  - Your new best friend! NSA tool, open source, audited for +1.5 years now.
  - Has a fucking decompiler!
- [IDA Pro]
  - $$$$$$$ but de facto standard for many years.
- [Radare2]
  - Cutter frontend, ghidra decomp. backend. Great community, arcane keybindings.
- [Binary Ninja]
  - Superb alternative if you don't mind spending a little (**student discounts apply**)
- [Hopper]
  - Great if you are on macOS, not too expensive.
- [Objdump]
  - Caveman tool, still very useful
- [gdb]
  - Get some extensions for gdb to make it nicer!
  - [peda]
  - [gef]
  - [pwndebug]

More tools (A tier)

- [apktool] - Unpack android applications
- [jadx] - Java reversing GUI environment.
- [JEB] - Premium Java reversing suite (and more). but $$$$$
- [Capstone] - Multi-arch dissasembly framework.
- [Unicorn] - Really nice emulation engine.
- [Volatility] - Memory forensics tool.
- [Qira] - Timeless debugger with a nice GUI. Not the best maintained project.
- [angr] - Constraint solver
- [z3] - Theorem solver / constraint solver
- [hxd] - nice hex editor

Windows specific tools

- [Windbg]
- [x64dbg]
- [Scylla]
- [OllyDbg]
- [ProcessHacker]
- [PEiD]
- [PeStudio]
- [dnspy]
  - .NET stuff

Resources

- Ghidra [https://ghidra-sre.org/]
- IDA/Hex-Rays [https://www.hex-rays.com/]
-
-
  [https://blog.rchapman.org/posts/Linux_System_Call_Table_for_x86_64/]
- [https://cs.brown.edu/courses/cs033/docs/guides/x64_cheatsheet.pdf]