# Reverse Engineering

## Tools:

* Objdump
* Radare2
  + Disassembler, debugger and patching
  + Never write a debug at the same time
  + R2 binary
  + R2 -w binary
  + R2 -d binary
  + Aaa
    - Decode names
  + Pdf
    - Used after aaa
    - Pre disassembly function
  + Pd 20
    - 20 is Number of bytes/ instructions
* Afl
* GHIDRA
* GDB
  + Debugger
  + Use GEF to extend capabilities
  + Break \*main run
  + Break \*main+58 continue
  + Delete breakpoint 1 stepi
  + Need to deference a pointer by using the “\*”
* Hopper
  + Disassembler
* Cutter
* IDA pro

Variables:

* Local – [RBP-xxx]
* Function arguments – [RBP +xxx]
* Global – [RIP+/xxx], [xxxx]
* Pointers – LEA RAX, [RAX]; MOV RAX, [RAX]
* Load effective address