Cheatsheet

GDB

help <command> - manual

start – run program and break on main

run – run program

info functions – list all functions

list <function\_name> - show source of function

disass <function\_name> - show disassembly of a function

disass /m <function\_name> - disass function interleaving it with relevant C code

break \*<address or name> - set a breakpoint

info breakpoints – list breakpoints

manage breakpoints:

delete <bp\_number>

disable <bp\_number>

enable <bp\_number>

explore registers:

info registers

$(gdb)> i r

Info registers <reg\_name>

Examine/Print:

$(gdb)> p/F <address/symbol>

$(gdb)> x/NUF <address/symbol>

Where:

* N – number of units we want to examine
* U – units size, possible are:
  + b – byte
  + h – half word (2 bytes)
  + w – word
  + g - giant word (8 bytes)
* F – output data format:
  + x – hex
  + d – decimal
  + u – unsigned decimal
  + i – instruction
  + s – string
  + c – char

Examples:

x/32b $rsp - Get 32 bytes at address pointed by RSP:

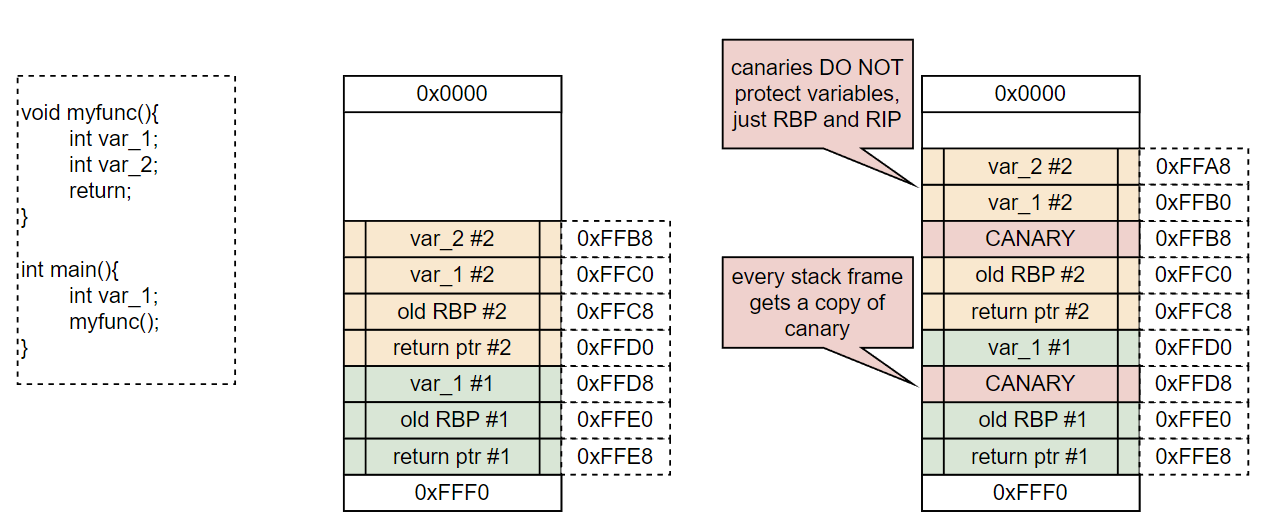
x/4gx $rsi - Get four 8-byte long values as hex at address from RSI

p/x $rsi - Print the value of RSI as hex

p/d 0x42424242 - Convert hex to decimal

Stack

Stack frame layout with and without canary



Basic overflow

