WHAT DOESN'T WORK:

INSIDE GDB

buf → 0x100

shell code

ret | 0x100

GDB stuff {

call stack

works OK

OUTSIDE GDB

buf → 0x100 + ???

shell code

ret | 0x100

call stack

does not work!

notice: no GDB stuff in stack!
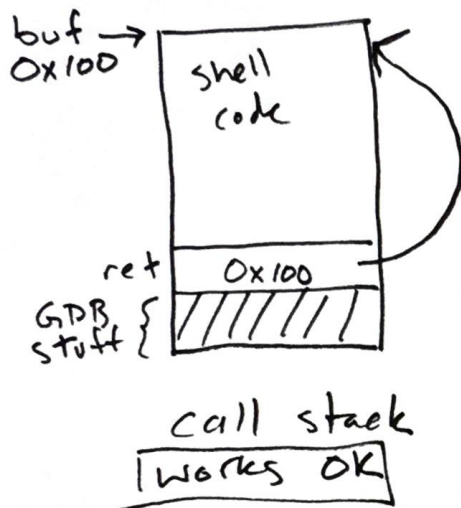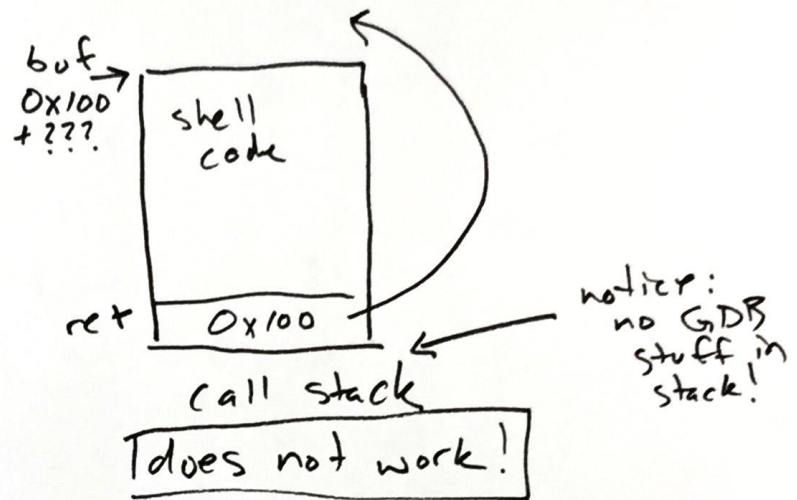
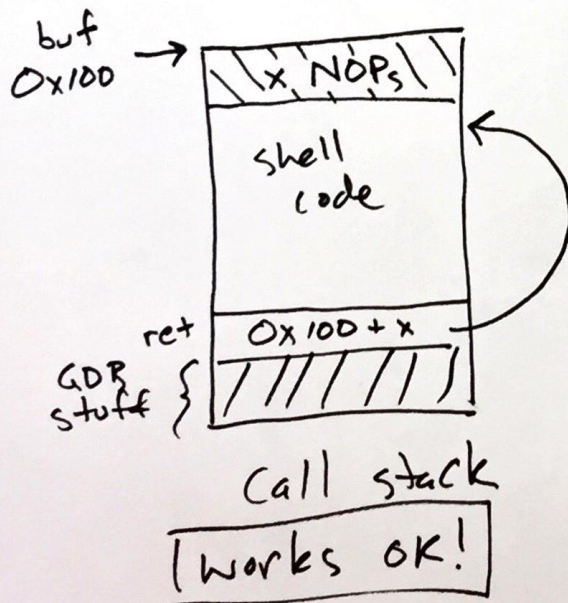# WHAT DOES WORK:

INSIDE GDB

buf → 0x100

x NOPs

shell code

ret | 0x100 + x

GDB stuff {

call stack

works OK!

OUTSIDE GDB

buf → 0x100 + x

x NOPs

ret | 0x100 + x

call stack

works OK!
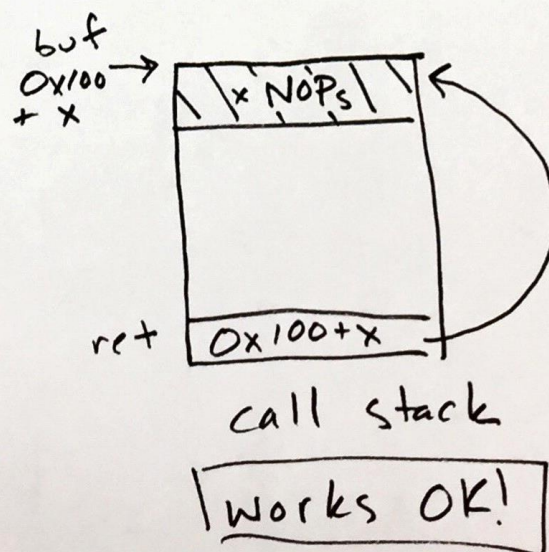
NOTE THAT: if $x \geq |\text{"GDB stuff"}|$ then the program will always "return" inside the NOP sled and the exploit will work in/out of GDB.