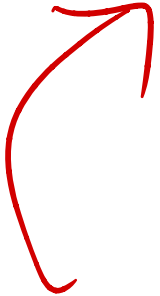
CS 208

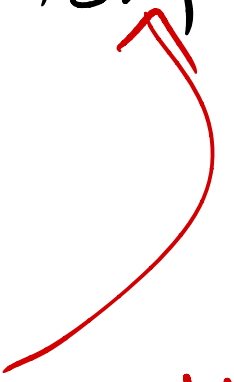
M, 27 Oct 2025

Remember: what does call do?

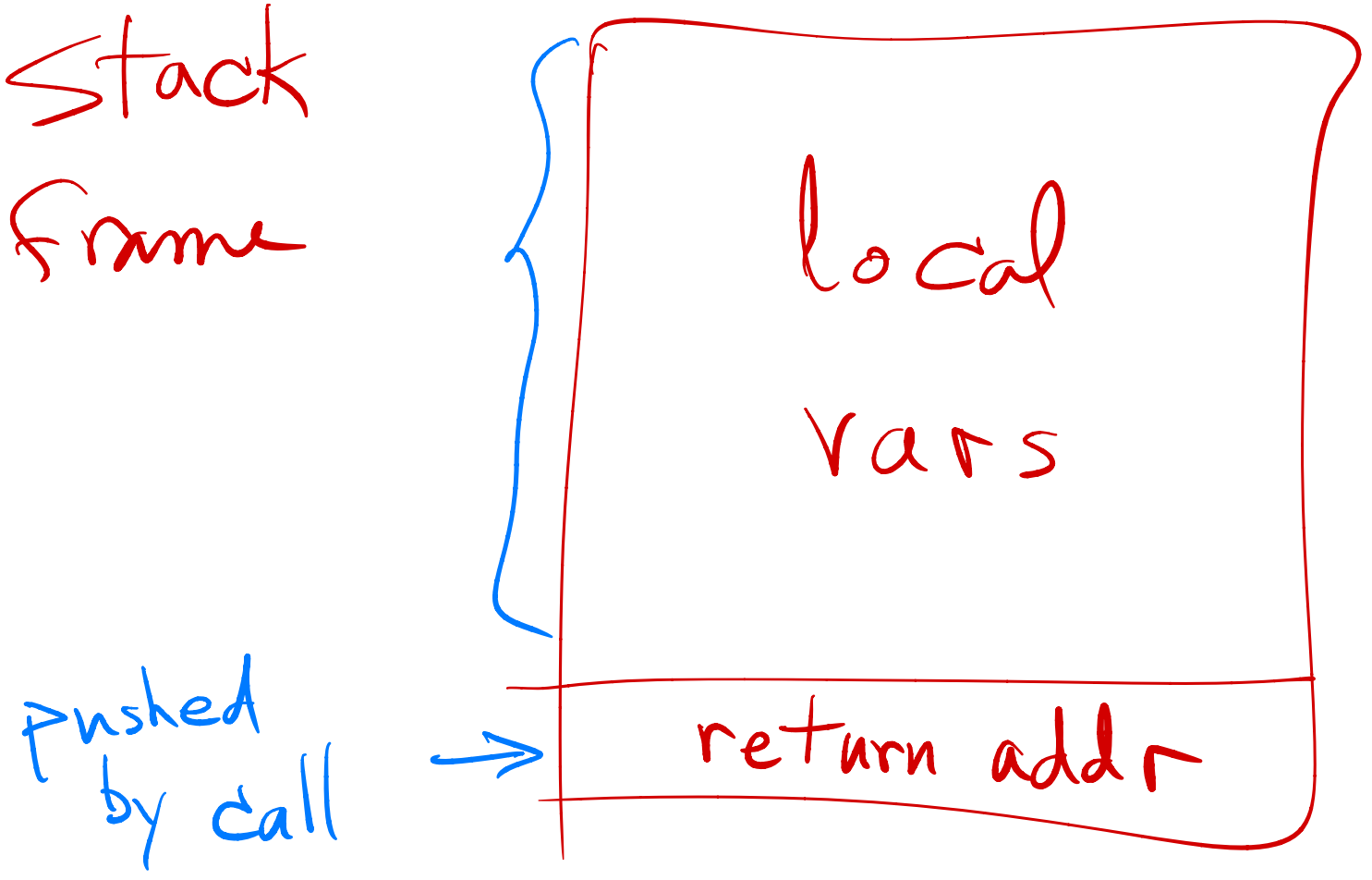
- push the return address
- jump to the function



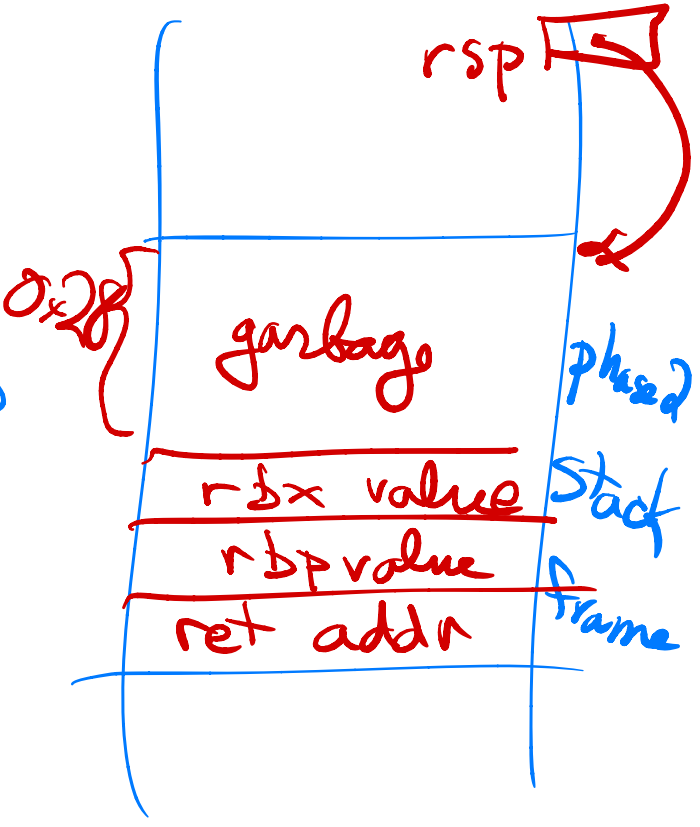
rsp = rsp - 8
ret addr goes to $rsp



rip = addr of function


Stack
frame
local
vars
pushed
by call
return addr

phase_2

save mains copies of rbp & rbx { push %rbp
push %rbx

make space for local vars { sub 0x28, %rsp