CS 208

M, 19 Feb 2024

0x401609 call 0x40183a <Gets>

0x40160e

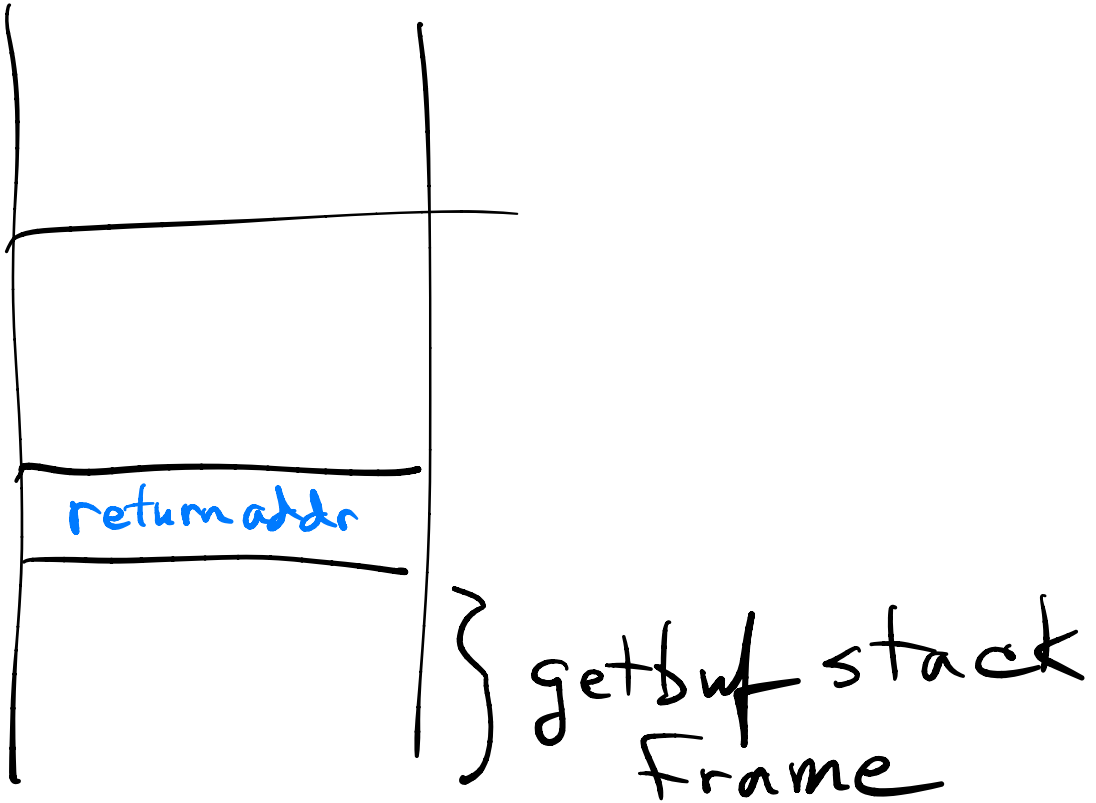
---

rsp = rsp - 8

"*rsp" = 0x40160e ← 8 bytes

rip = 0x40183a } jump to the function

save (push) the return address


return addr
getbuf stack
frame

retq

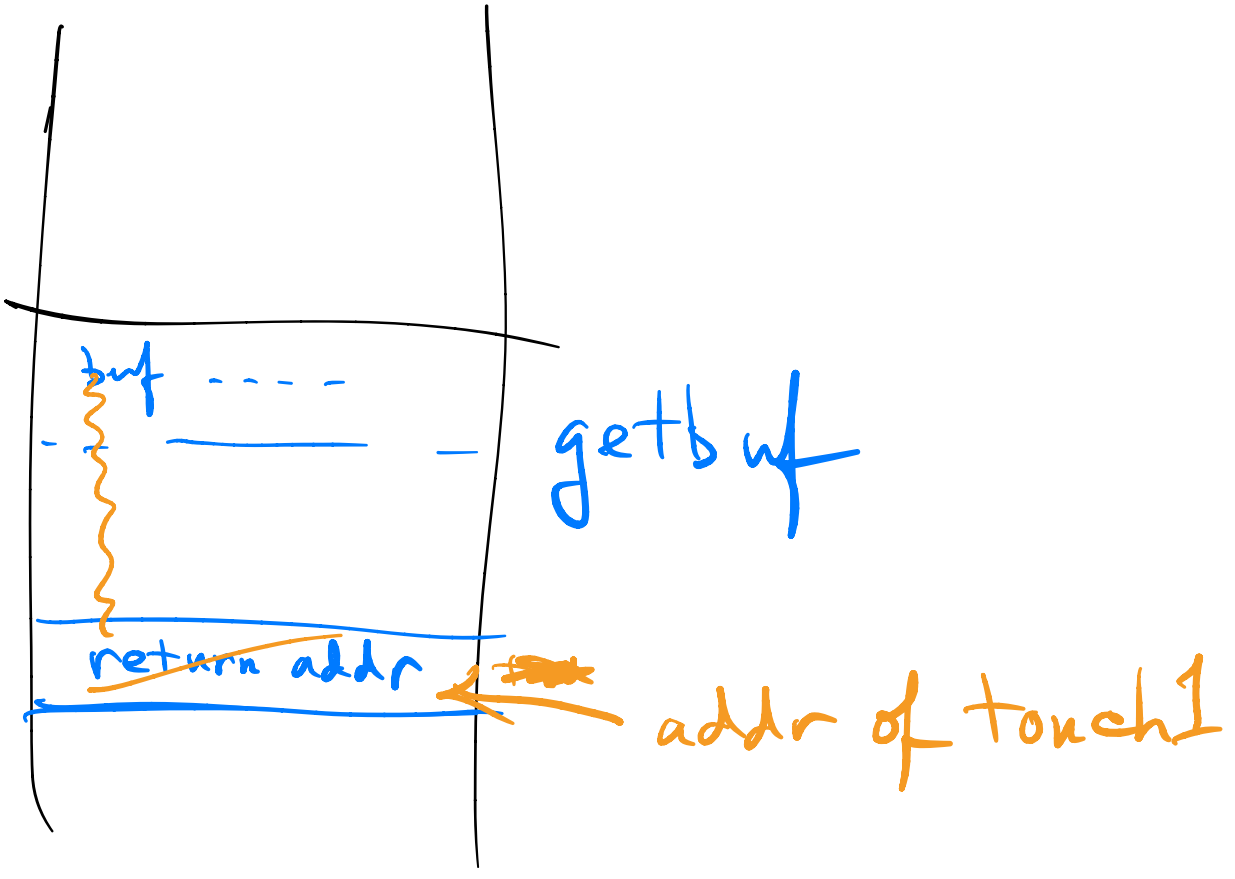
---

rip = "*rsp"

rsp = rsp + 8

} pop & jump

phase 1



phase 2 & 3