(記憶體)

ebp是存取參數或變數之基準點

main.s

✓ 1992: movl ②$8, 4(%esp)

✓ 1996: movl ③$5, (%esp)

✓ 2000: call ④ _add

2004: movl %eax, 28(%esp) 返回位址.

movl ⑫ 28(%esp), %eax

13 存入.

add.s

3000: (④ _add:) 標記不暫留

⑤ 保存ebp.

eip. (PC) → 3000: push %ebp

3004: ⑥ movl %esp, %ebp

3008: ⑦ movl 8(%ebp), %edx a 5

300C: ⑧ movl 12(%ebp), %eax b 8

3010: ⑨ addl %edx, %eax eax = eax + edx 13 5

3014: ⑩ popl %ebp 返回原保存的ebp

300B: ⑪ ret

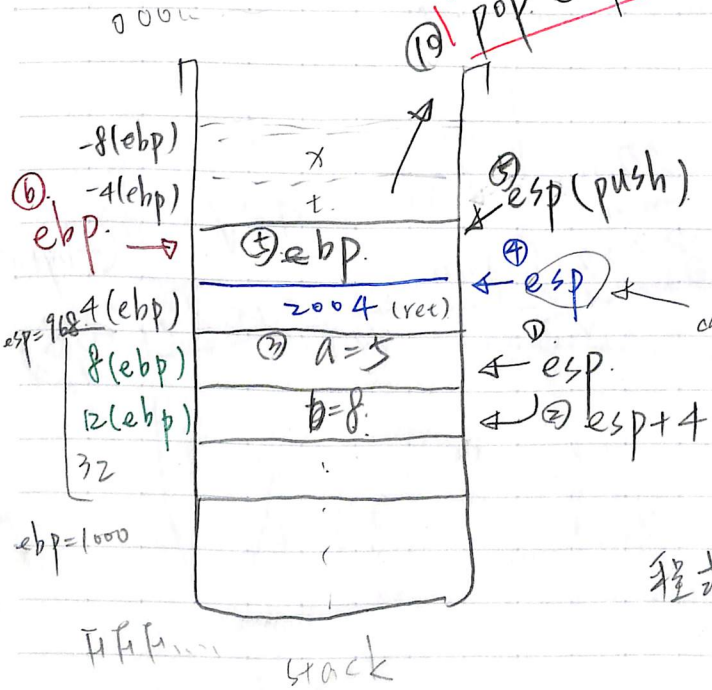
step1: pop address (2004)

step2: jmp.

(main).

恢復原本的基準點

⑩ pop ebp



call, push, pop, return 才會改變

程式設計師的自我修養