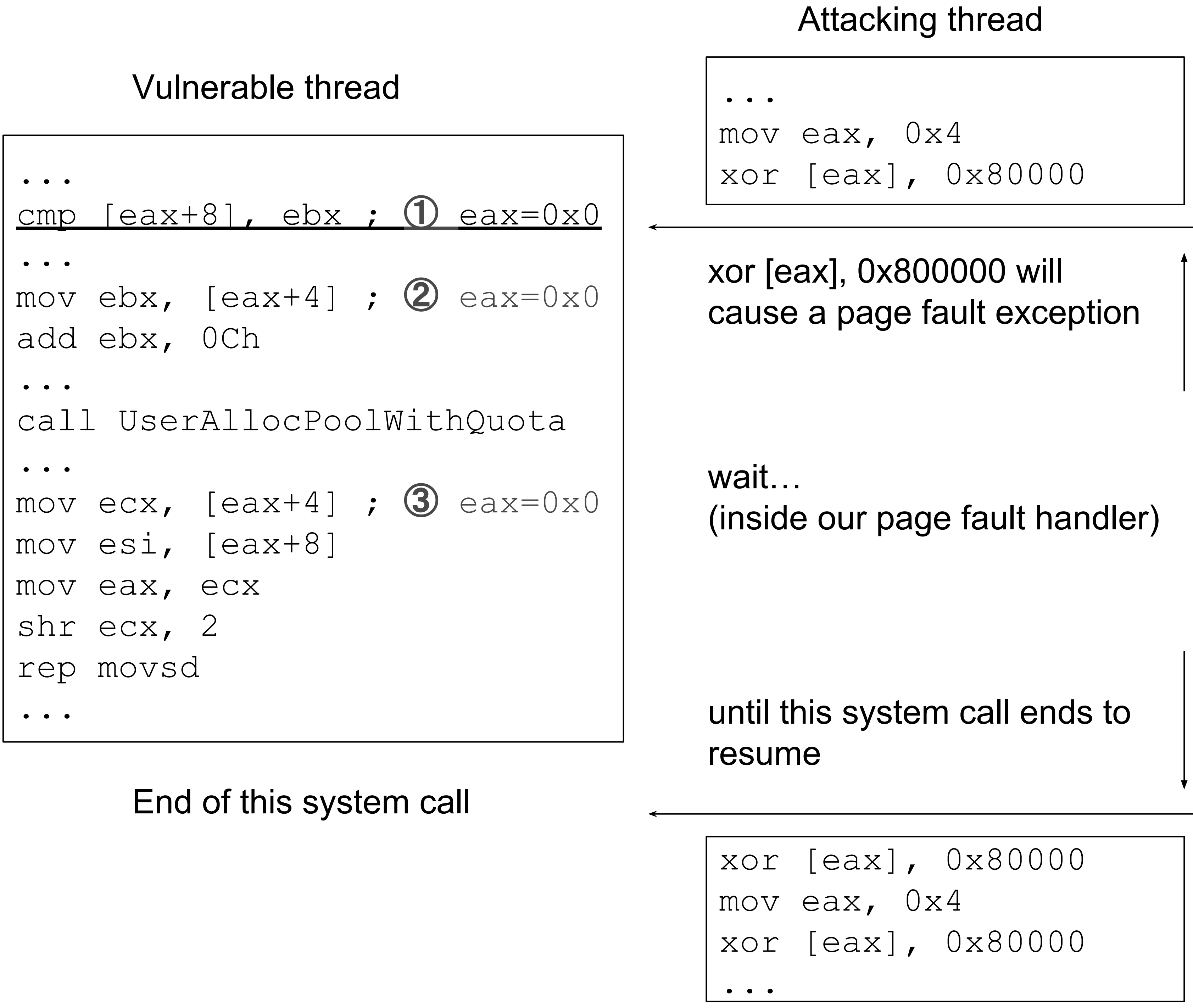

Attacking thread

```
...
mov eax, 0x4
xor [eax], 0x80000
```

Vulnerable thread

```
...
cmp [eax+8], ebx ; ① eax=0x0
...
mov ebx, [eax+4] ; ② eax=0x0
add ebx, 0Ch
...
call UserAllocPoolWithQuota
...
mov ecx, [eax+4] ; ③ eax=0x0
mov esi, [eax+8]
mov eax, ecx
shr ecx, 2
rep movsd
...
```

xor [eax], 0x800000 will cause a page fault exception

wait…
(inside our page fault handler)

until this system call ends to resume

End of this system call

```
xor [eax], 0x80000
mov eax, 0x4
xor [eax], 0x80000
...
```