Mem. Safety-related vulnerability

↓

Code Pointer Overwrite
(Control Data)

↓

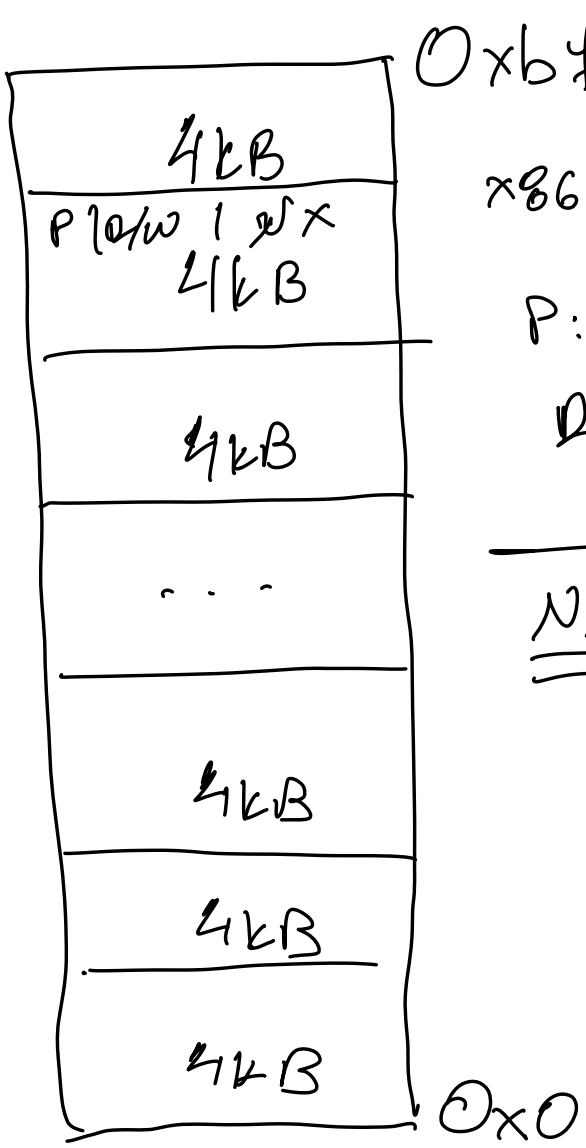
Control-flow Hijacking

↓

Code Injection

↓

Arbitrary Code Execution



x86 page size: 4kB

P: present

R/W: read, read/write.

NX

Mem. Safety-related vulnerability

↓

Code Pointer Overwrite
(Control Data)

↓

Control-flow Hijacking

↓

~~Code Injection~~ Non-executable mem.

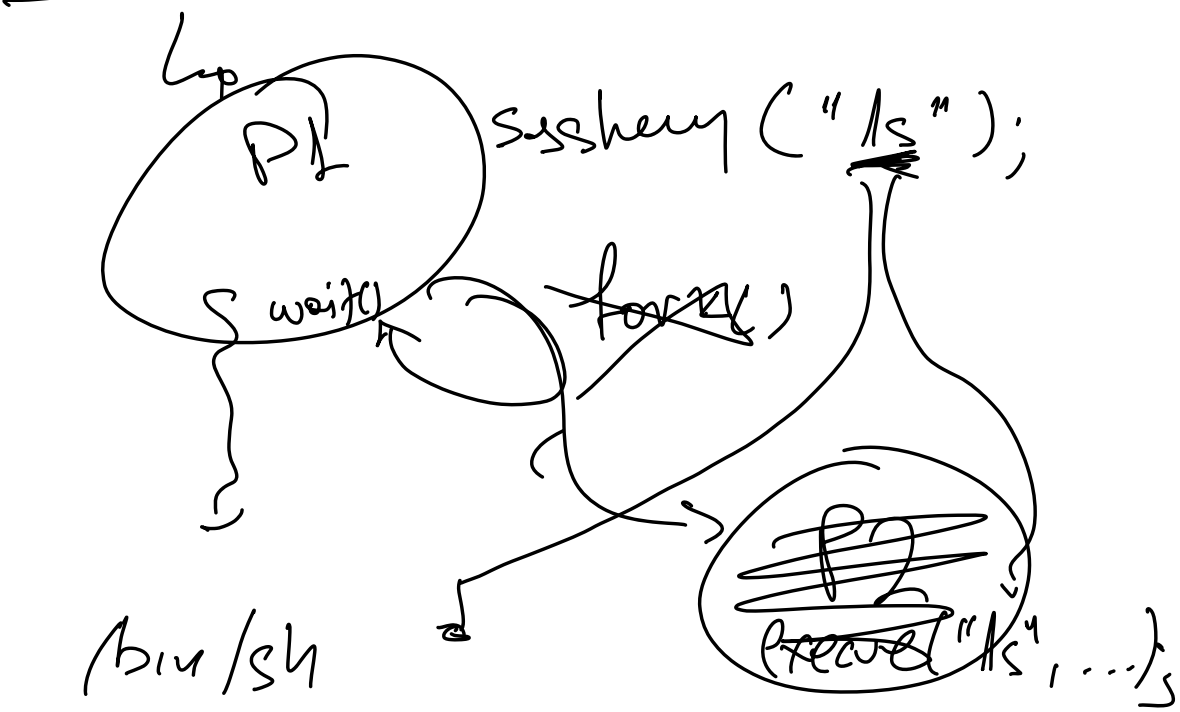
↓

Arbitrary Code Execution

Code Reuse

- Ret2libc
  (whole function reuse)

system("ls")



Mem. Safety-related vulnerability

↓

Code Pointer Overwrite
(Control Data)

↓

Control-flow Hijacking

↓

Code Injection ~~Non-executable mem.~~

↓ Code Reuse / ret2libc

Arbitrary Code Execution