Mem. Safety-related vulnerability

Code Pointer Overwrite (Control Data)

Control-flow Hijacking

Code Injection

Arbitrary Code Execution
x86 page size: 4 kB

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

L�ret2libc

(whole function reuse)
system("ls")

if
switch
for

/bin/sh

exec("ls", ...)
Mem. Safety-related vulnerability

Code Pointer Overwrite (Control Data)

Control-flow Hijacking

Code Injection [NON-EXECUTABLE MEM]

Code Deuse/ref2lib

Arbitrary Code Execution