Address Space Layout Randomization (ASLR)

- Partial: Stack, unmap, heap
- Full: partial + exec.
Address Space Layout Randomization (ASLR)

- partial: stack, inner heap
- full: partial + exec.

Requires PIC

Position Independent Code

- no absolute addresses (in code)
- data
- code
Memory Disclosure Vuln.

To read/leak memory contents (ideally arbitrary)

vs.

Memory Corruption Vuln.

To write/alter memory contents (ideally arbitrary)
Memory Disclosure Vulnerability

- to read/leak memory contents (ideally arbitrary)

vs.

Memory Corruption Vulnerability

- to write/alter memory contents (ideally arbitrary)

- can be abused to construct new disclosure values.