# ASLR - Address Space Layout Randomization

- The OS randomize the location (random offset) of the stack, the heap and the standard libraries

- Harder for the attacker to guess buffer addresses and the address of a lib-c subroutine

- Disabling ASLR protection on Linux
  `$ sysctl kernel.randomize_va_space=0`

- Bypassing ASLR protection :
  - Brute-force attack to guess the ASLR offset
  - Get the offset with targeted data leak

# PIC/PIE - Position Independent Code/Executables

- **Without PIC/PIE**
  library or code is compiled with absolute addresses and must be loaded at a specific location to function correctly

- **With PIC/PIE**
  library or code is compiled with relative addressing that are resolved dynamically when executed by calling a function  to obtain the return value on stack

- Disabling PIE protection on Linux
  `$ gcc ...-z -no-pie`

➡ Works complementarily of the ASLR