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

Confined execution environment - Sandbox

A sandbox is tightly-controlled set of resources for untrusted programs to run in

➡ Sandboxing servers - virtual machines

➡ Sandboxing programs

- Chroot and AppArmor in Linux
- Sandbox in MacOS Lion
- Metro App Sandboxing in Windows 8

➡ Sandboxing applets - Java and Flash in web browsers