ASLR

- The OS randomize the location (random offset) where the standard libraries and other elements are stored in memory

- Harder for the attacker to guess 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

- Bypassing ASLR protection : *Return-Oriented-Programming (ROP)* exploit use instruction pieces of the existing program (called "gadgets") and chain them together to weave the exploit

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