

# CTF 정보보안 콘테스트 챌린지북

## 202L2H

# Chap5 = pwn! pwn! pwn!

## 주소 노출

# ASLR

- Heap, Stack, mmap (공유 라이브러리)
- 실행 파일이 위치하는 주소는 랜덤화되지 않는다.
- 주소가 고정된 범위 안에서 **eip**를 잘 제어해서 원하는 영역의 주소를 추출하는 것이 목표.