

# 1 Kernel

## 1.1 Compilation

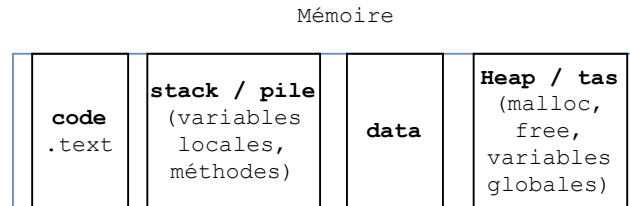
On configure avec `make linux-menuconfig` (ou `make linux-xconfig`) puis on lance une compilation avec `make linux-rebuild`

## 1.2 Busybox

Busybox est un exécutable qui combine beaucoup de fonctions de base (ls, mv, rm, cat, etc...). En mettant toutes ces commandes dans un seul programme, on réduit énormément les redondances et par conséquent la taille de l'exécutable.

On peut également configurer busybox avec `make busybox-menuconfig` puis le compiler avec `make busybox-rebuild`

## 1.3 Attaques



**Exécution sur le stack** : Si le stack est exécutable, il est possible d'y placer du code puis de l'exécuter (ce qui est de moins en moins le cas).

### 1.3.1 ret2libc

Permet de bypasser la non-exécution du stack. Consiste à exécuter du code dans une librairie comme libc.

### 1.3.2 ROP