ASLR

1. ASLR

ASLR(Address Space Layout Randomization,随机地址空间分配)，通过加载程序的时候不再使用固定的基址加载，从而干扰shellcode的定位

（1）映像随机化

映像随机化是在PE文件映射到内存时，对其加载的虚拟地址(VA)进行随机化处理，这个地址是在系统启动时确定的，系统重启后这个地址会变化，但只随机化了前2个字节

（2）堆栈随机化

这项措施是在程序运行时随机的选择堆栈的基址，与映像基址随机化不同的是堆栈随机化不是在系统启动的时候确定的，而是在打开程序的时候确定的

（3）PEB与TEB随机化

不再使用固定的PEB基址0x7FFDF000和TEB基址0x7FFDE000