ASLR地址空间随机化

2025年3月4日 13:55

地址空间随机化(Address Space Layout Randomizaion,ASLR)：OS用来抵御缓冲区溢出的内存保护机制，使得在OS上运行的进程内存地址无法被预测。

- 只有在编译时作为位置无关可执行文件(PIE)的可执行程序才能得到ASLR对的最大保护，其.exe的所有代码节区会被加载到随机地址，PIE机器码不管绝对地址是多少都可以正确执行。
- 64位下最佳，但是达不到2^64，因为内核和用户空间，也包括ALSR及PIE的启用会占据一部分，留给mmap和brk的可分配区域大约42T。
- 通过随机放置进程关键数据区域的地址空间来防止攻击者能可靠地跳转到内存的特定位置来利用函数，防范恶意程序对已知地址进行Return-to-libc攻击（用来对抗不可执行栈的攻击，绕过栈保护机制，通过缓冲区溢出来获取权限）
- 在Linux系统下的进程模型中，代码段/BSS/全局数据区应该是不变的；加载的依赖库的代码位置/栈空间/堆空间可能会变。(存疑)
- 实现方法应该有两种：全局ASLR和局部ASLR，全局ASLR对整个系统的内存地址随机化，而局部ASLR仅对特定进程或库进行随机化。（存疑）

X86-64基本分布：

-	-
内核地址空间范围	[0XFFFF 0000 0000 0000, 0XFFFF FFFF FFFF FFFF]
用户地址空间	[0X0000 7FFF FFFF F000, 0X0000 0000 0000 0000]
不规范地址空间	不属于内核或者用户的地址空间属于不规范地址空间

用户空间大小由宏定义TASK_SIZE决定，这个大小默认为128T对应0X0000 7FFF FFFF F000

mmap的起始计算为:STACK_TOP - 栈最大长度 - 间隙 - 随机值。栈最小长度为128M随机位数配置在/proc/sys/vm/mmap_rnd_bits default=28默认随机最大值为 0xFFFFFFF000 大约为1T，用户空间起始地址0x7FFFFFFFF000。

ELF文件如果是普通的EXEC类型则会使用指定的入口地址下面讨论PIE编译出的DYN可执行文件
其加载地址为 DEFAULT_MAP_WINDOW /32上增加一个arch_mmap_rnd随机值
DEFAULT_MAP_WINDOW /32 = 0x555555554AAA同mmap一样为 0x00FFFFFFF000 约1个T大小。代码段起始位置约为84T 随机值 1T。

假定编译出来的是PIE类型的ELF并且全开ASLR设置那么在mmap和heap之间的地址空间大小

大约是
128T - 1T - 84T - 1T = 42T
mmap最小起始地址略小于0x0000 7F00 0000 0000，brk起始地址最大略大于 0x0000 5655 5555 5555。考虑到计算时忽略了一些小的单位(GB级别或者更小), 包括间隙 小的随机值, 以及动态库 数据段代码段本身占用的空间, 这里可以做一个进一步的保守计算来使用这个空间。计算这个空间的意义在于, 例如我们对共享内存使用一个固定的地址时, 需要避免和系统本身的动态分配的地址空间相冲突, 而计算出来的地址空间的确定可以保证这一点,。

某些情况下可以绕开ASLR防护

- 如果缓冲区足够大，当希望跳转至缓冲区中执行指令时，可以尝试通过大量填充 NOP 使得跳转成功的机率增加。但这种方法要求苛刻，成功率低，偏暴力。
- 某个寄存器中的值刚好指向了我们需要的地址。
- 通过某些方式泄露出动态库的加载地址。
- 2016 年的Jump Over ASLR论文指出，可以利用分支指令通过旁路探测出模块加载的地址，这篇文章的大概后面会简单讲一下。

内核同样可以开启ASLR，在Linux中被称为KASLR，它随机化内核在虚拟空间中的地址，只有内核自己知道我在哪，别人不知道。但是在熔断和幽灵漏洞出现后 KASLR 不再安全。目前 KASLR 已被 KPTI（内核页表隔离）所取代。

引用:

1、ASLR 是如何保护 Linux 系统免受缓冲区溢出攻击的 - 知乎
2、地址空间布局随机化ASLR的深入探讨：实现、影响与挑战_YNXZ的技术博客_51CTO博客
3、Linux内核内存保护机制：aslr和canary - 真昼小天使daisuki - 博客园
4、linux内存布局和地址空间布局随机化（ASLR）下的可分配地址空间_linux地址随机化哪几部分-CSDN博客
5、腾讯QQ&TIM本地提权POC(CVE-2023-34312) | CN-SEC 中文网
6、Linux下的ASLR（PIE）内存保护机制和绕过 | 运维开发绿皮书
7、栈缓冲区溢出之二 ASLR | dontpan1c 的 CTF 笔记