

calloc 有以下特性

不会分配 tcache chunk 中的 chunk 。

tcache 有以下特性

在分配 fastbin 中的 chunk 时若还有其他相同大小的 fastbin\_chunk 则把它们全部放入 tcache 中。

思路

题目给了 backdoor 函数，只要全局变量 ptr 中有值，就会执行 system("/bin/sh") ,所以我们解题思路很明确，就是往 ptr 中填值。具体步骤如下：

首先分配 8 个 0x80 大小的 chunk ，依次 free 掉，这样 tcache 中 0x80 的 chunk 列表已经被填满，还多了一个 0x80 的 chunk 在 fast bin 中。

分配一个 0x80 大小的 chunk ，这个 chunk 会从 tcache 中取出，这一步的目的是为了在 tcache 留出空位。

类似 fastbin attack ，将 fastbin 里的 chunk 的 fd 指针改为 ptr - 0x10 处，这样 calloc 将这个 chunk 分配出去时，就会认为 fd 指针对应的也是一个 chunk ，会把这个 chunk 放入 tcache ，而 tcache 中是以 fd 指针连接的，这样 ptr 的值就会被修改为某个 fd 的指针。这样我们就能执行 system('/bin/sh') 拿 shell 了。