Windows平台的rop exp编写

转载

山清水秀iOS 于 2016-08-10 10:40:00 发布 62 收藏
原文链接：http://www.cnblogs.com/Ox9A82/p/5755805.html

摘抄自看雪

Windows的ROP与Linux的ROP并不相同，其实Linux下的应该叫做是ret2libc等等。Windows的ROP有明确的执行目标，比如开辟可执行内存然后拷贝shellcode，比如释放可执行执行文件然后执行等等，总之要依赖于一些关键的Windows API来进行。

进行ROP的目的：绕过DEP保护

ROP gadgets：是以 ret 指令结尾的连续的指令

查找gadgets的算法：

1. 搜索所有的ret指令
2. 向前遍历，判断ret的前几个字节是否为合法指令。保留能构成有效指令的最大字节数20 bytes。记录这些指令序列。

常见的功能性gadgets：

- 赋值寄存器：如：pop eax;ret;
- 从内存读：如：mov ecx,[eax];ret;
- 向内存写：如：mov [eax],ecx;ret;
- 数学运算：如：add eax,0x0b;ret;
- 系统调用：如：int 0x80;ret;

避免使用的gadgets：

- 用包含leave的 gadgets，会导致栈祯不可控
- 用包含pop ebp的 gadgets，会导致栈祯不可控

转载于:https://www.cnblogs.com/Ox9A82/p/5755805.html