SCTF2014_pwn400 writeup

转载

weixin_30765577 于 2016-09-09 14:34:00 发布 38 收藏
文章标签： 大数据 python 数据结构与算法
原文链接：http://www.cnblogs.com/fancystar/p/5856558.html


```
int sub_804874A()
{
  unsigned __int8 v1; // [sp+1Fh] [bp-9h]@2

  write(1, "1.New note\n", 0xBu);
  write(1, "2.Show notes list\n", 0x12u);
  write(1, "3.Show note\n", 0xCu);
  write(1, "4.Edit note\n", 0xCu);
  write(1, "5.Delete note\n", 0xEu);
  write(1, "6.Quit\n", 7u);
  write(1, "option--->> ", 0xCu);
  do
    v1 = getchar();
  while ( v1 == 10 );
  return v1;
}
```

函数作用：
1.新建一个note。
2.遍历note。
3.查看note，会输出note的首地址。
4.编辑note的content，其中将输入的内容strcopy到content中发生溢出。
5.删除一个note，双向链表的指针更改时，可以实现DWORD SHOOT。

note结构：
4字节：指向自己的指针
4字节：flink
4字节：blink
64字节：title
32字节：type
256字节：content

delete函数：

```
ptr = (_DWORD *)strtol((const char *)&buf, 0, 16);// ptr=输入的node地址
if ( (_DWORD *)*ptr == ptr )
{
  if ( *(_DWORD **)a1 == ptr )
  {
    *(_DWORD *)a1 = *(_DWORD *)(*(_DWORD *)a1 + 8);// node=node->blink
  }
  else if ( ptr[2] )
  {
    v1 = ptr[2];                        // v1=node->blink
    v2 = ptr[1];                        // v3=node->flink
    *(_DWORD *)(v2 + 8) = v1;           // node->flink->blink=node->blink
    *(_DWORD *)(v1 + 4) = v2;           // node->blink->flink=node->flink
  }
  else
  {
    *(_DWORD *)(ptr[1] + 8) = 0;        // node->flink->blink=0
  }
  write(1, "succeed!\n\n", 0xAu);
  free(ptr);
```

free()成为shellcode跳板

思路：
要卸载中间note，所以先建立3个note。（其实两个也行，将第一个note的content伪装成note头）
在建立第三个note时将shellcode写入content。
布置要卸载的note的头部（自身地址、flink中写入shellcode地址、blink中写入free()got表地址）

我将node2的content布置为node头部
l32(ptr2+108)+l32(ptr3+108)+l32(free_got_addr-4)

ptr2+108 为node2的content起始地址
ptr3+108 为node3的content起始地址，即是shellcode地址

```
.got.plt:0804A450 off_804A450     dd offset free
0804A450  98 A4 04 08
```

```
extern:0804A498 ; void free(void *ptr)
extern:0804A498                 extrn free:near
```

找到GOT表中free()函数指针
v1+4=free_got_addr
*(free_got_addr)=shellcode__addr
v1=free_got_addr-4

exp: https://github.com/Minxin/exploit/blob/master/SCTF2014_pwn400.py

转载于:https://www.cnblogs.com/fancystar/p/5856558.html