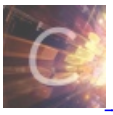
others_shellcode

原创

m0sway 于 2022-03-30 11:41:49 发布 81 收藏

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



others_shellcode

使用`checksec`查看：

只留了一个Canary，栈不可执行和PIE都开了。

先放进IDA中分析：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  getShell();
  return 0;
}
```

- `getShell();`：主函数中直接给了后门函数，跟进查看。

`getShell();`：

```
signed int getShell()
{
  signed int result; // eax

  result = 11;
  __asm { int     80h; LINUX - sys_execve }
  return result;
}
```

- `__asm { int 80h; LINUX - sys_execve }`：直接`syscall 80`拿权限了。

题目思路

- 直接连接就能拿到权限。

步骤解析

> 无需

完整exp

```
from pwn import *

#start
r = process("../buu/others_shellcode")

#params

#attack

r.interactive()
```