

week1-xiaoheshang

test_nc

直接nc一下

ls看到了flag

cat flag

easy_overflow

```
xiaoheshang@xiaoheshang-virtual-machine:~/desktop$ checksec vuln
[*] '/home/xiaoheshang/desktop/vuln'
Arch:      amd64-64-little
RELRO:     Partial RELRO
Stack:     No canary found
NX:        NX enabled
PIE:       No PIE (0x400000)
```

找到backdoor

```
f deregister_tm_clones
f register_tm_clones
f __do_global_ctors_aux
f frame_dummy
f b4ckd0or
f main
f __libc_csu_init
f __libc_csu_fini
f _term_proc
f system
```

这题出现了close1比较新颖，之前没有遇到过

close 1: 把标准输出关了

可以用execv 1>&0打开就可以正常了

sign in

base64

直接线上找一个解码的

test your IDA

打开ida

直接能够找到flag