**实验1** 完成64位目标程序roarctf\_2019\_realloc\_magic的利用。

**实验目的：**

* + 学会64位堆UAF漏洞利用方法，结合pwntools编写利用脚本，得到本地shell [粘贴脚本截图和shell截图]
  + 掌握Tcache Attack
  + 掌握stdout 泄露libc地址的方法
  + 掌握劫持free\_hook的方法

**实验题目：**

1. 完成roarctf\_2019\_realloc\_magic题目，通过堆漏洞利用，拿到本地shell。







