

实验信息

pwn手应该觉得没什么压力，除了不用pwntools可能不太适应。

👉 基本信息

缓冲区的溢出实验，程序写的挺麻烦的，不过可以直接通过函数找到关键部分：

```
000000004017A8  .text: 000000004017A8  ; __unwind {
000000004017A8  .text: 000000004017A8  sub     rsp, 28h
000000004017AC  .text: 000000004017AC  mov     rdi, rsp          ; dest
000000004017AF  .text: 000000004017AF  call    Gets
000000004017B4  .text: 000000004017B4  mov     eax, 1
000000004017B9  .text: 000000004017B9  add     rsp, 28h
000000004017BD  .text: 000000004017BD  retn
000000004017BD  .text: 000000004017BD  ; } // starts at 4017A8
000000004017BD  .text: 000000004017BD  getbuf
000000004017BD  .text: 000000004017BD  endp
000000004017BD  .text: 000000004017BD  .-----
```

思路：

控制输入字节长度从而控制返回地址0x0000000004017C0。

第二个就是在第一个的基础上布置参数，让参数等于cookie值：写一段汇编可以搞定,但是如果是在ubuntu 1604上面的话，会有aslr 和 nx等保护，代码注入可能8太行，rop可解决。

Copy Code

```
1  movq    $0x59b997fa, %rdi
2  pushq   0x4017ec
3  ret
```

c >

第三个的话不过是比第二个改成了字符串输入。

其余的就是比较简单的rop攻击

👉 预习准备

👉 课堂录音

【💡 点击最左侧的“+”，选择“附件音频与录制”功能，一边听课一边实时录音，遇到重点随时打标记】

👉 课堂讲义

【💡 点击最左侧的“+”，选择“附件”功能，将老师的课件文件作为附件进行上传，便于随时查看】

👉 课堂记录

👉 拓展资料


影像资料

网页书签

添加网页书签，了解更多信息，拓展视野，方便查阅。

印象笔记 | 工作必备效率应用

作为你的第二大脑，印象笔记可以帮助你简化工作、学习与生活。你可以在手机、电脑、平板、网页等多种设备和平台间，无缝同步每天的见闻、思考与灵感。快速保存微信文章、微博、网页等内容，一站

 <http://Yinxiang.com>

【💡 点击最左侧的“+”，选择“网页书签”功能，将相关课程资料链接粘贴在对话框中，即可插入链接，便于随时查看】