

**信息系统安全上机实验报告**

题目：信息系统安全威胁示例

**学生姓名 石子跃**

**学生学号 3020244294**

**学院名称 智算学部**

**专 业 网络空间安全**

**时 间 2023-02-26**

目 录

[第一章、实验目的 1](#_Toc20510)

[第二章、实验原理 2](#_Toc5686)

[第三章、实验环境 3](#_Toc4806)

[第四章、实验步骤 4](#_Toc12927)

[第五章、实验结果分析 5](#_Toc19785)

[第六章、实验说明 1](#_Toc19785)0

### 

1. 实验目的

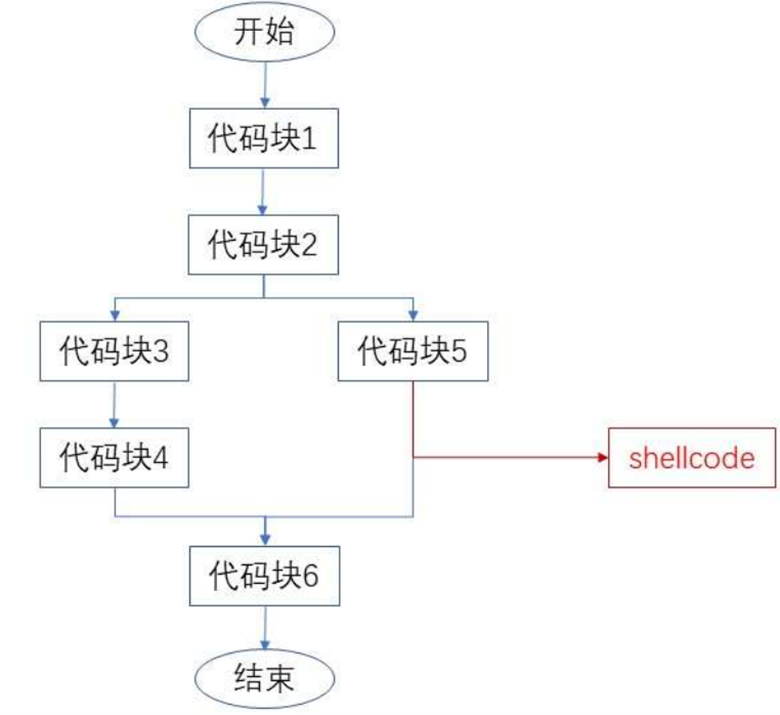
信息系统安全在现实中的安全威胁示例很广泛，安全威胁基于的技术手段也种类多样。为了更好的了解这些安全威胁为信息系统带来的危害性，要求自研一种安全威胁示例，实验环境可控，非真实攻击。

实验小组选取的内容是shellcode的原理介绍和简单的shellcode攻击原理复现。

1. 实验原理

实验使用了在新生赛比赛中出现的shellcode题目，首先对shell与shellcode进行介绍，shell是一个使用C语言编写的程序，是用户使用Linux的桥梁。Shell 是指一种应用程序，这个应用程序提供了一个界面，用户通过这个界面访问操作系统内核的服务。Shellcode 是一段可以执行特定功能的特殊汇编代码，在设备漏洞利用过程中注入到目标程序中从而被执行。Shellcode原意指获取到shell的代码，现在泛指利用过程中获得控制权后执行的代码。

在比赛中，使用控制流劫持可以对目标程序的执行过程以及下一步执行目标进行修改，这样的话在获取到控制权后，shellcode就可以执行他的功能。控制流劫持主要强调执行控制权，而shellcode更关注于有了控制权之后的功能。因此shellcode更像是控制流劫持的载荷，往往对于不同漏洞来讲控制流劫持是特殊的，因为控制流劫持需要考虑程序中存在的漏洞如何去利用，而shellcode会具有一些通用性，因为此时的控制权已经被获得了，shellcode只需要考虑如何去执行即可。



1. 实验环境

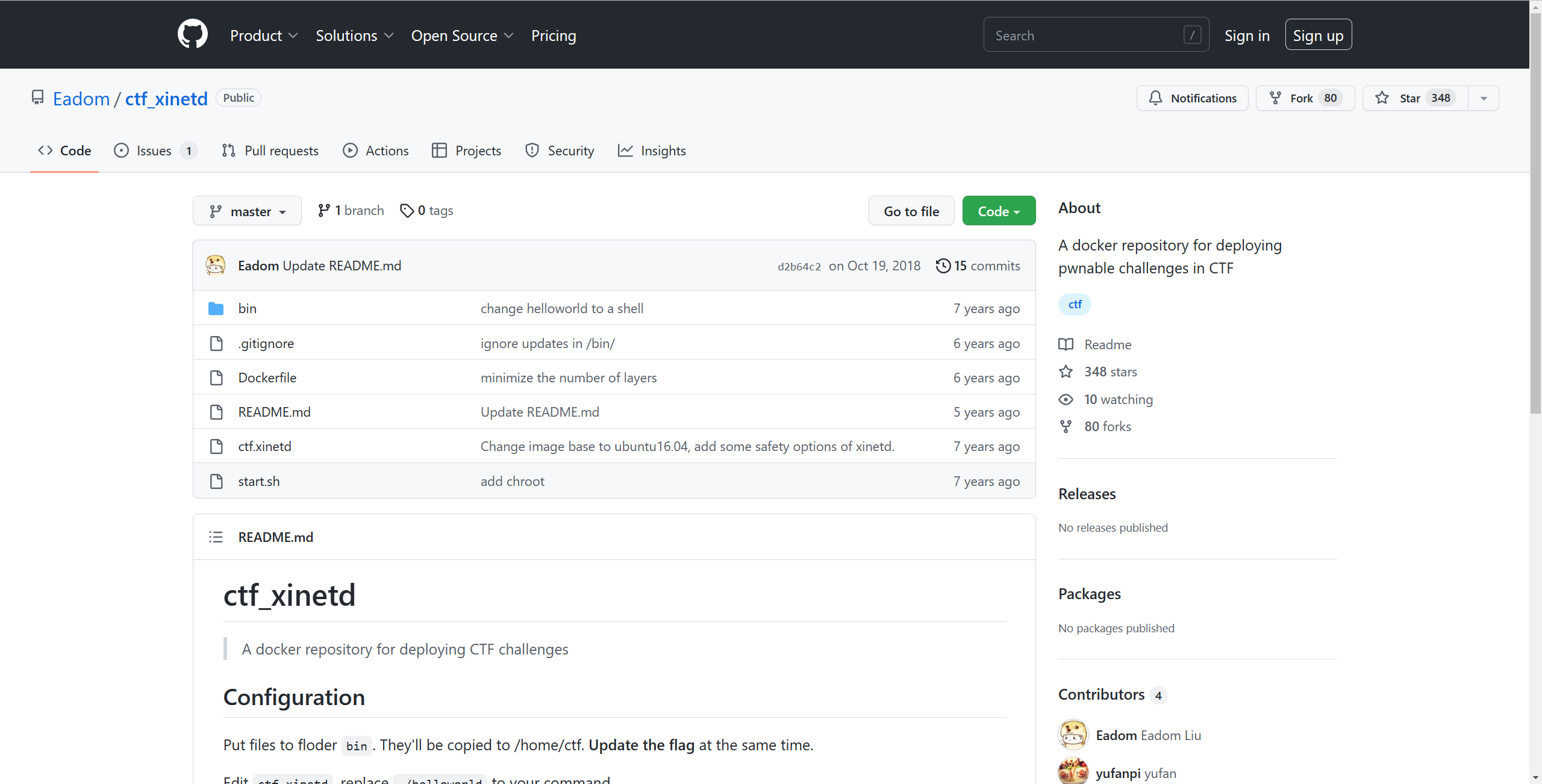
操作系统：Ubuntu16.04

使用题目：ret2shell

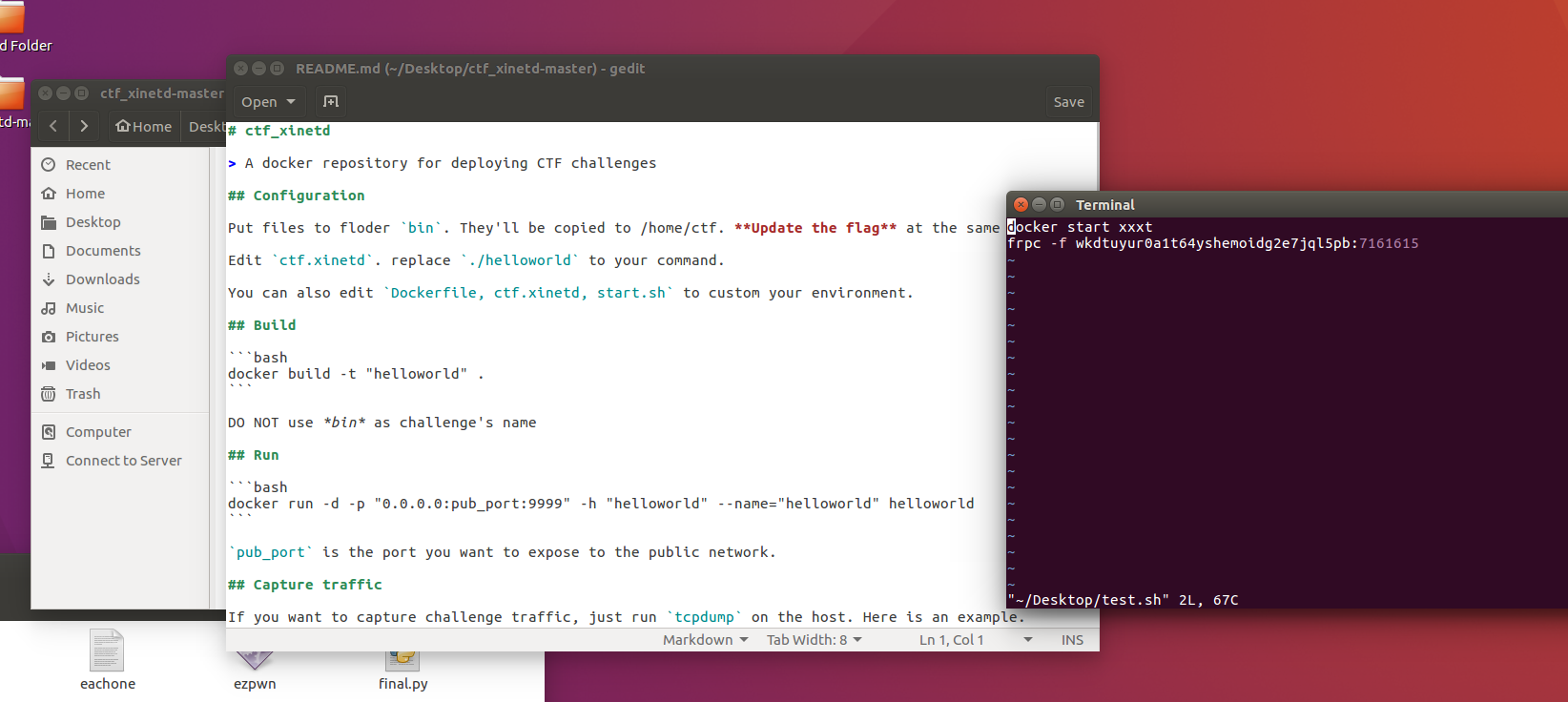
题目提供文件：ezpwn（二进制可执行文件，已经放到了靶机上）

靶机：使用Docker进行搭建的虚拟机环境

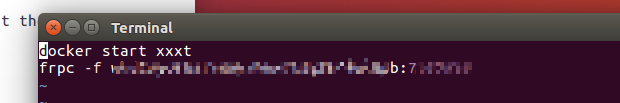
上网查找相关CTF靶场搭建项目：



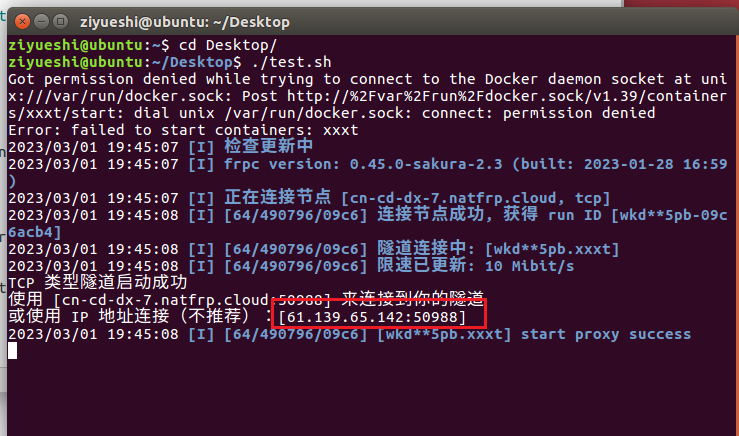
根据Readme.md文件进行自定义搭建，同时新建自己的flag信息：



编写.sh文件方便快速搭建，同时使用内网穿透工具将端口放在公网，方便其他计算机进行攻击操作：

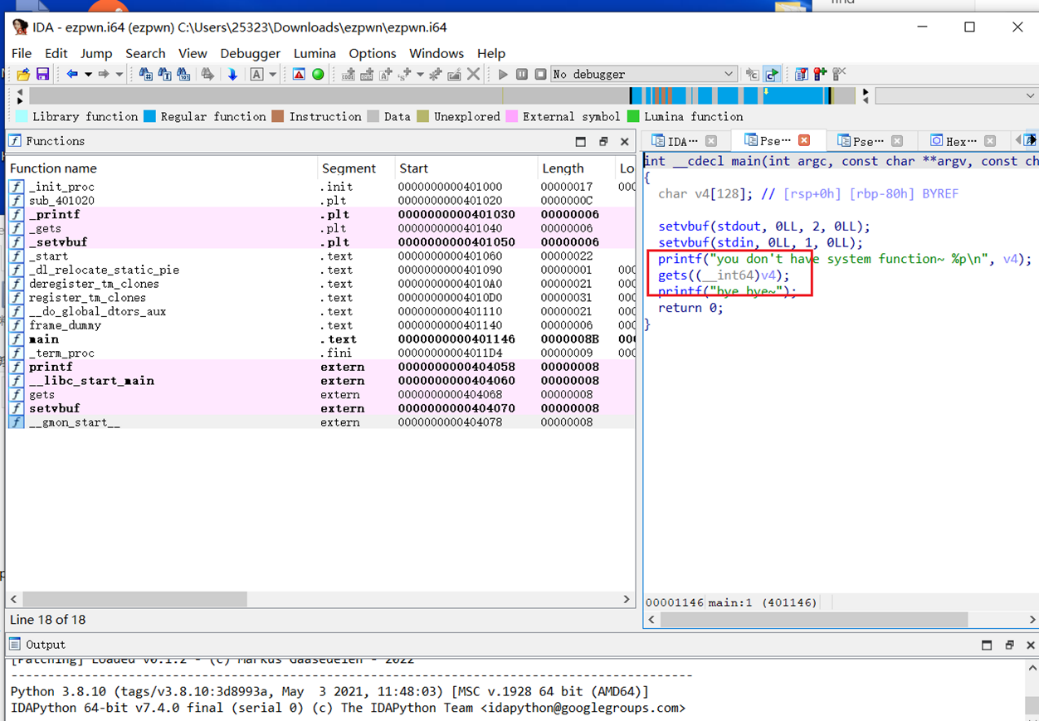


启动成功，利用图片内端口，开始实验：



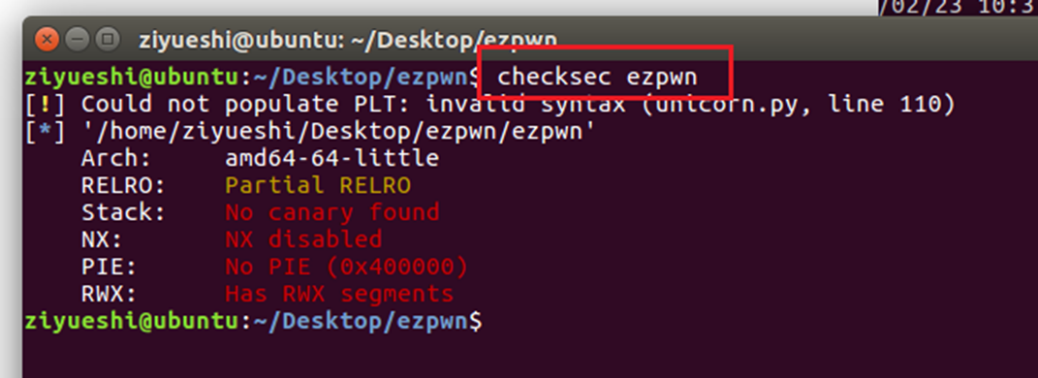
1. 实验步骤

获取到对应二进制文件后，使用IDA Pro对二进制文件进行分析，在反汇编后，查看源码中是否存在可以利用的漏洞：



可以发现，gets函数对变量v4进行了操作，也就是缓冲区会有一定的修改，同时在上一条语句中的printf中也有v4的出现，这个地方可以获取到v4的地址。

使用checksec命令对二进制文件进行检查，检查结果可以告诉我们，这个程序是存在很多对攻击有利条件的。例如在这个程序中，可以栈溢出，在可执行内存，没有开启ASLR地址随机化，同时也具备了可读写执行代码权限。



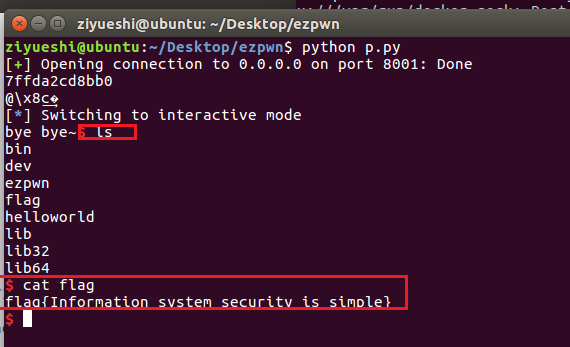
根据每次输出的V4数组的起始地址，进行shellcode的编写。利用脏字符填充，输入shellcode，覆盖原有的返回地址为shellcode的起始地址。从而执行shell，获取shell，并完成相关数据的读取。



1. 实验结果分析

运行结果：

查看攻击成功后获取的文件目录：



查看关键信息，攻击完成：

flag{Information system security is simple}

1. 实验说明