目录

[首先是准备实验环境 1](#_Toc150795340)

[下面尝试作业中的栈溢出原理： 3](#_Toc150795341)

[需要的环境有反汇编工具ida： 3](#_Toc150795342)

[Pwn安装问题： 3](#_Toc150795343)

[安装gef调试工具 8](#_Toc150795344)

[实验溢出栈溢出原理 8](#_Toc150795345)

[基本ROP ret2text 10](#_Toc150795346)

[知乎攻击 11](#_Toc150795347)

[ret2shellcode 11](#_Toc150795348)

首先是准备实验环境，需要32位环境，输入命令安装编译32位c程序的软件包：

sudo apt-get update

sudo apt-get install -y lib32z1 libc6-dev-i386 lib32readline6-dev

sudo apt-get install -y python3.6-gdbm gdb

最后一条有问题：Couldn‘t find any package by regex ‘python3.6‘

通过apt-get install的直接方式无法安装python，可以采用配置编译软件包的执行方式

手动安装python3.7：

1. 在终端中下载Python安装包：

下载地址：https://www.python.org/ftp/python/3.7.1/Python-3.7.1.tgz

命令：

wget https://www.python.org/ftp/python/3.7.1/Python-3.7.1.tgz

2. 解压Python安装包

tar xzvf Python-3.7.1.tgz

3. 安装Python某些模块所需要的依赖库：

sudo apt-get update

sudo apt-get install build-essential libncursesw5-dev libgdbm-dev libc6-dev zlib1g-dev libsqlite3-dev tk-dev libssl-dev openssl libffi-dev libbz2-dev -y

即

sudo apt-get dist-upgrade -y

sudo apt-get install build-essential python-dev python-setuptools python-smbus -y

sudo apt-get install build-essential libncursesw5-dev libgdbm-dev libc6-dev -y

sudo apt-get install zlib1g-dev libsqlite3-dev tk-dev -y

sudo apt-get install libssl-dev openssl -y

sudo apt-get install libffi-dev -y

若不安装依赖，会出现

ModuleNotFoundError: No module named ‘\_ctypes’

的错误

02 开始安装

1. cd到刚刚解压的Python路径中，然后运行命令：

./configure

2. 运行以下命令进行安装：

sudo make && sudo make install

四 验证

python3.7 --version

首先尝试了知乎中一个实验：<https://zhuanlan.zhihu.com/p/643817714>获取了管理员账户。

linux 系统中，/bin/sh 实际是指向 /bin/bash 或 /bin/dash 的一个符号链接。为了重现这一防护措施被实现之前的情形，我们使用另一个 shell 程序（zsh）代替 /bin/bash。下面的指令描述了如何设置 zsh 程序：  
注意**实验系统未安装zsh，如安装可跳过第一条命令**

sudo apt install zsh

sudo su

cd /bin

rm sh

ln -s zsh sh

exit

## 下面尝试作业中的栈溢出原理：

需要的环境有反汇编工具ida：

用ubutun中的Firefox浏览器找到：<https://www.hex-rays.com/products/ida/support/download_freeware/>

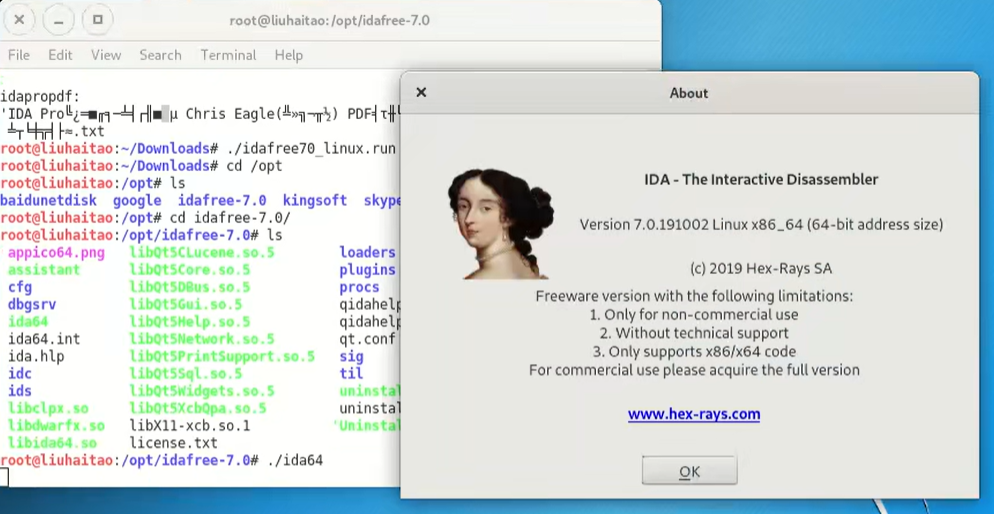
下载安装包。

到下载位置运行./idafree…开始安装，安装到opt/下的ida。。。。中。

到opt/idafree。。。文件下运行ida64

需要qt的运行环境：

sudo apt install libxcb-xinerama0



选择文件即可开始反汇编。

Pwn安装问题：

1. ubutun里同时有python2.7和python3.7该如何将环境改成python3的环境：

如果您想将 Ubuntu 系统的默认 Python 环境更改为 Python 3，可以按照以下步骤进行操作：

1. 确认 Python 版本：
   * 运行 python --version 查看默认的 Python 版本。
   * 运行 python3 --version 查看 Python 3 版本。
2. 更新软件包列表：

复制

sudo apt update

```

1. 安装 Python 3：

复制

sudo apt install python3

```

1. 设置 Python 3 为默认版本：

复制

sudo update-alternatives --install /usr/bin/python python /usr/bin/python3 1

```

1. 验证更改：
   * 运行 python --version 确认默认的 Python 版本是否为 Python 3。
2. 安装pwn：

要在 Ubuntu 上安装 pwntools，您可以按照以下步骤进行操作：

1. 确保您的系统上已经安装了 Python 2.7 或 Python 3。您可以通过运行以下命令来检查：

复制

python --version

或

复制

python3 --version

1. 确保您的系统上已安装 pip 工具。pip 是 Python 的包管理器，用于安装 Python 包。您可以通过运行以下命令来检查：

复制

pip --version

或

复制

pip3 --version

如果未安装 pip，请使用以下命令安装 pip：

复制

sudo apt-get install python-pip

或

复制

sudo apt-get install python3-pip

1. 使用 pip 安装 pwntools。运行以下命令来安装 pwntools：

复制

pip install pwntools

或

复制

pip3 install pwntools

1. 验证安装。运行以下命令来验证 pwntools 是否成功安装：

复制

python -c "import pwn; print(pwn)"

或

复制

python3 -c "import pwn; print(pwn)"

1. 在执行pip3 install pwntools命令后出现了错误：Command "python setup.py egg\_info" failed with error code 1 in /tmp/pip-install-y9mkka96/MarkupSafe/

You are using pip version 10.0.1, however version 23.3.1 is available.

You should consider upgrading via the 'pip install --upgrade pip' command.

这个错误可能是由于缺少一些依赖项或其他配置问题导致的。您可以尝试以下解决方法：

1. 升级 pip：  
   根据错误信息提示，您可以尝试升级 pip 到最新版本。运行以下命令来升级 pip：

复制

pip install --upgrade pip

```

或

pip3 install --upgrade pip

1. 安装依赖项：  
   pwntools 可能需要一些依赖项才能正常安装。运行以下命令来安装它们：

复制

sudo apt-get install python3-dev libffi-dev build-essential

```

1. 清理缓存：  
   在安装过程中，有时会出现缓存问题，可以尝试清理 pip 的缓存并重新安装 pwntools。运行以下命令来清理缓存：

复制

pip3 cache purge

1. 执行pip3 install --upgrade pip时出现：Could not install packages due to an EnvironmentError: [Errno 13] Permission denied: '/usr/local/bin/pip3'

Consider using the --user option or check the permissions.

该错误提示表明您在执行升级 pip 的命令时遇到了权限问题。这可能是由于您没有足够的权限来修改 /usr/local/bin/pip3 文件。

使用 sudo：  
如果您有管理员权限，可以使用 sudo 命令来提升权限，以便执行升级 pip 的命令。运行以下命令：

shell

复制

sudo pip install --upgrade pip

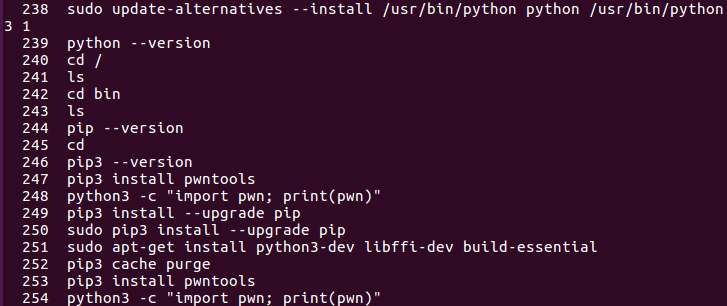
1. 有了依赖，更新了pip3，重新安装pwn工具

pip3 install pwntools

python3 -c "import pwn; print(pwn)"  
<module 'pwn' from '/home/admain-rose/.local/lib/python3.7/site-packages/pwn/**init**.py'>

该输出表明成功导入了 pwn 模块，并显示了模块的路径 /home/admain-rose/.local/lib/python3.7/site-packages/pwn/\_\_init\_\_.py。这表明 pwntools 已经位于您的 Python 3.7 的包目录中

1. 目前为止命令：



Pwntools还需要依赖six：

Pip3 install six

还需要在path中添加six组件和pwn组件的位置six在前面：

export PYTHONPATH="${PYTHONPATH}:/usr/lib/python3/dist-packages"

export PYTHONPATH="${PYTHONPATH}: /home/admain-root/.local/lib/python3.10/site-packages"

安装gef调试工具

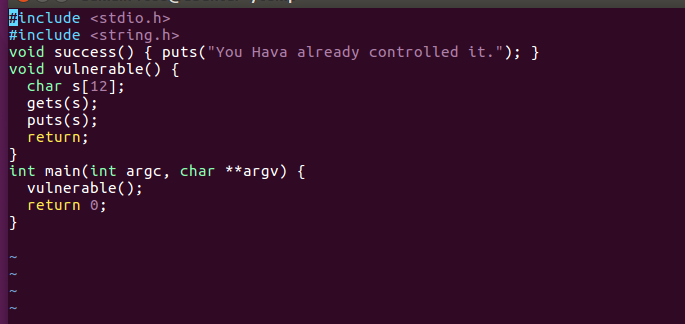
https://github.com/hugsy/gef

$ wget -O ~/.gdbinit-gef.py -q https://gef.blah.cat/py

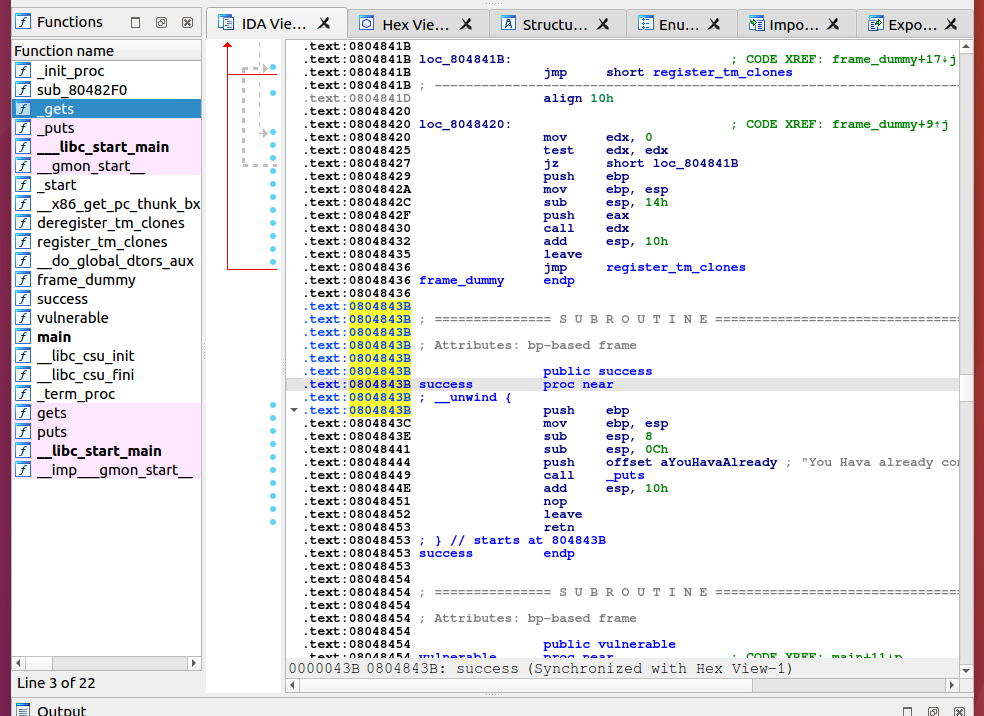
$ echo source ~/.gdbinit-gef.py >> ~/.gdbinit

注意：先把~/下的gdbinit和gdbinit-gef.py删除再执行上面两行程序

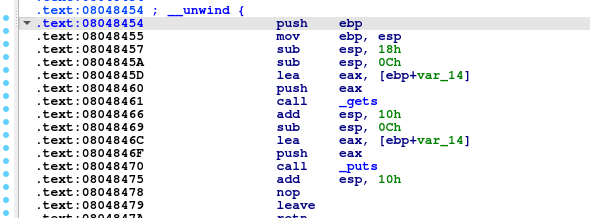
实验溢出栈溢出原理



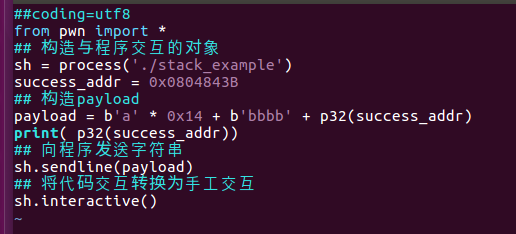
Stack-eample源码



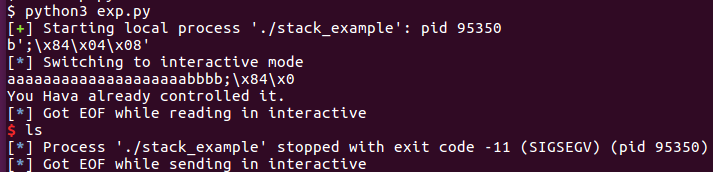
Stack-example反汇编结果，可以看到success的地址为：0x084843B



包含get的函数时ebp+14h，所以填满14h的数组，加上一个4Bpush ebp，下面的4B就是该函数的返回地址，把这个地址填成success的地址就行。

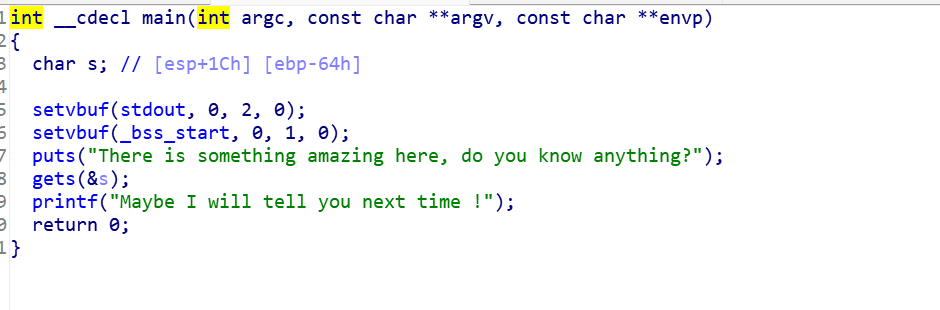


这是攻击用的python，用的时python3的代码，需要把success\_addr改掉。然后运行python3 exp.py就可以得到结果



基本ROP ret2text

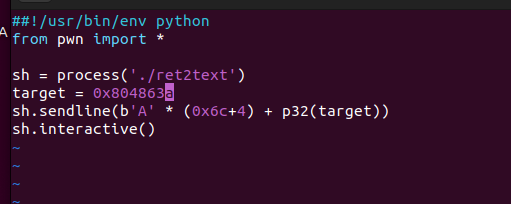
在宿主机上用IDA查看源代码



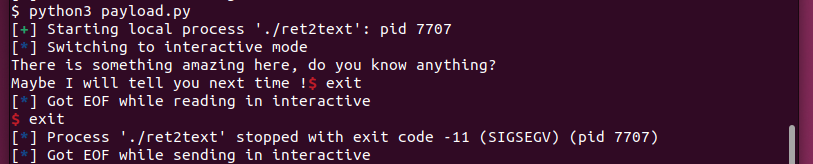
用gef在call处设置断点，查看寄存器值：



由esp-eax=0x6c可得payload：



执行payload可得攻击得手截图：



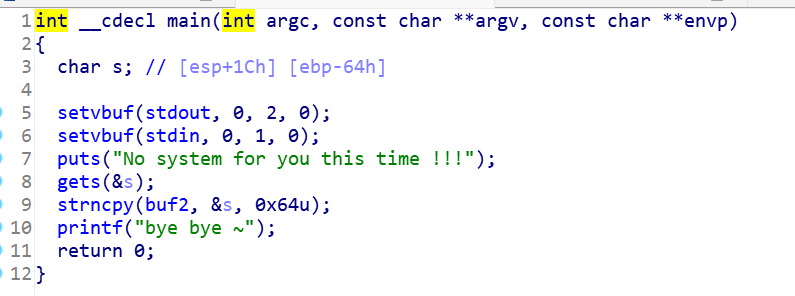
知乎攻击

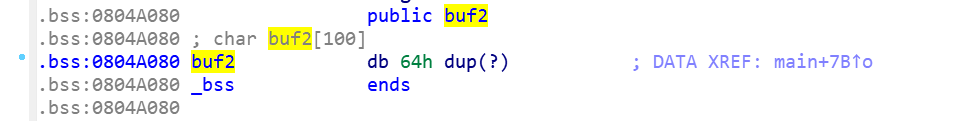
<https://zhuanlan.zhihu.com/p/643817714>

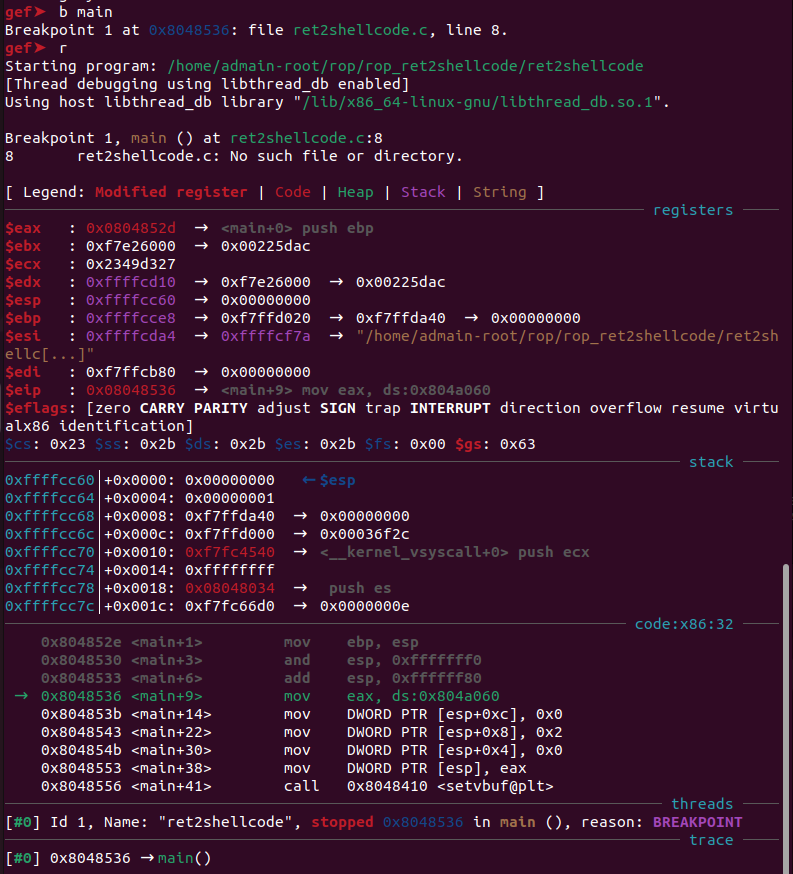
之后再试

ret2shellcode

反汇编结果，以及buf2放到了可执行区域







下面看一下buf2区域是否可执行



好像不能执行？有问题

ret2syscall