乱七八糟的pwn入门（一）——环境搭建

原创

Z_Pathon 于 2019-08-05 13:22:37 发布 406 收藏 8
分类专栏： 乱七八糟的pwn入门 文章标签： pwn入门 环境搭建 学习笔记

本文链接：https://blog.csdn.net/Z_Pathon/article/details/98475434

- **前言**

首先，这不是教程，只是对我学习过程的记录，我也是新手，有些地方一知半解，所以难免有错误和疏漏，因此不可全信，也请路过的大佬们不吝赐教，感激不尽。

为啥说是乱七八糟呢，是因为我的基础在于本科学过一些操作系统、汇编、内存分析的课程。但是大学课程嘛，基本只有概念，只会个皮毛。自学过一点点python和linux命令，也只有看过书，基本没操作过，所以实践起来基本靠现用现搜。那些大佬们推荐的书也就停留在见过书名，躺在购物车的状态。只是凭着兴趣想要自己学习和摸索一下，所以整体的思路和过程会比较乱，但是我会尽量写的详细一点，感觉会比较适合那些像我一样只了解了pwn的概念就一门心思想尝试的萌新们。

之前被大佬推荐了一个学习pwn的网站——*pwnable.kr*，这个网站就是像游戏一样，有好多关卡，都是从简单到复杂的pwn题目。大佬在博客里写了writeup，我的学习过程也是打算基本按照大佬的博客走，学习一下大佬的思路，膜拜大佬传送门：https://etenal.me/archives/972

- **万里长征第一步——环境搭建**

下面进入正题，手把手教你如何搭建pwn的环境（大佬教的，我就负责传个话），这个过程是当时大佬发在群里的，比他博客里的要流畅一点（因为没有报错）。

首先，准备一个干净的ubuntu16的系统（亲测ubuntu18不行，因为它有些依赖的版本太高），可以去官网下，因为我直接在电脑上装的系统，所以没有配置虚拟机的操作；

然后，不要有任何多余操作，直接Ctrl-Alt-t打开终端，输入下面几条指令：

1.备份默认源：

```
sudo cp /etc/apt/sources.list /etc/apt/sources.list.old
```

源：就是ubuntu系统的软件、库等等的来源；

sources.list：是存放系统源列表的文件；

sudo：给用户root权限的命令，相当于拿到了系统的尚方宝剑，用途很多，这里是为了对高冷的系统文件进行操作；

cp：不是组cp的cp，是copy的cp，就是复制粘贴。

2.修改源列表文件的权限：

```
sudo chmod 777 /etc/apt/sources.list
```

chmod：修改文件或目录权限的命令，后面三个数字分别是给user、group、other的权限，其中，读权限为4、写权限为2、执行权限为1。需要哪些权限直接把对应数字相加即可，7就是有读、写、执行权限，这样就可以在下一步修改文件的内容，

3.清空默认源：

```
sudo cat /dev/null > /etc/apt/sources.list
```

cat /dev/null > 文件名：就是专门清空文件内容的命令，cat命令的作用类似于文档内容的转移。

4.添加源：

就是往sources.list文件里添加下面的内容：

```
deb https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ xenial main restricted universe multiverse
# deb-src https://mirrors.tuna.tsinghim.edu.cn/ubuntu/ xenial main main restricted universe multiverse
deb https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ xenial-updates main restricted universe multiverse
# deb-src https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ xenial-updates main restricted universe multiverse
deb https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ xenial-backports main restricted universe multiverse
# deb-src https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ xenial-backports main restricted universe multiverse
deb https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ xenial-security main restricted universe multiverse
# deb-src https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ xenial-security main restricted universe multiverse
```

这里用的源是清华大学的源，有两种方法可以完成添加的操作：

第一种是直接打开/etc/apt文件夹，找到sources.list文件，右键用gedit打开，直接复制粘贴（好用但不高端）；

第二种是在终端输入：

```
sudo vi /etc/apt/sources.list
```

vi：是系统自带的编辑器，和后面要用的vim一样，用专用的命令进行操作。

然后按i进入编辑模式，复制上述代码后，右键粘贴（不要用Ctrl-v）。之后，

Esc-->输入：-->输入wq-->回车。

wq：vi和vim的命令，就是保存并退出。

5.更新源：

```
sudo apt-get update
```

6.安装必要软件：

```
sudo apt-get install vim
sudo apt-get install git
sudo apt-get install build-essential checkinstall
sudo apt-get install libreadline-gplv2-dev libncursesw5-dev libssl-dev libsqlite3-dev tk-dev libgdbm-dev li
```

别问那么多，装就对了（问了俺也不知道）。

7.安装gdb-peda：

```
cd ~
git clone https://github.com/longld/peda.git ~/peda
echo "source ~/peda/peda.py" >> ~/.gdbinit
echo "DONE! debug your program with gdb and enjoy"
```

同上

8.如果你是64位系统，那么需要安装32位libc：

```
sudo apt-get install gcc-multilib
```

好像是某些依赖要用到，别问，问就是只管装。

9.恭喜你到了最后一步，安装pwntools：

```
sudo apt-get install python2.7 python-pip python-dev git libssl-dev libffi-dev
pip install --upgrade pwntools
```

pwntools：一个pwn常用的python库，它有好多功能可以让代码更简洁，同时也简化了过程，这些功能就在后面的使用里慢慢探索吧。

- **本章总结**

啰啰嗦嗦了一大堆，终于写完了。搭环境嘛，也没啥好总结的，主要就是熟悉一下linux命令行的操作吧。

最后，就祝各位搭环境顺利吧～