My\_Ubandu\_Pwn\_VmFile

也算一个demo吧！

折腾了几天，还是用的Ubandu16.04的版本。之前用的Ubandu18的版本，总是有问题。然后还有一些东西没有完善之后陆续完善，但是，初期的pwn题是可以做了。

首先先感谢CSDN上面的giantbranch，因为之前一直用的这位大佬的虚拟机。然后再感谢CTF-Wiki给的配置虚拟机的思路。

虚拟机名字isidro 密码toor Root的密码也是toor

可以passwd改用户密码 可以sudo passwd root改Root密码

2019/8/7下面写我的虚拟机配置，后续会更加完善

0x0 Ubandu和pip换源

**$ cd ~ && mkdir .pip**

**$ cd ~/.pip && touch pip.conf**

**$ sudo nano pip.conf**

**写入下面的内容:**

**[global]**

**index-url = https://pypi.tuna.tsinghua.edu.cn/simple**

**[install]**

**trusted-host=mirrors.aliyun.com**

**$ sudo apt-get update**

**$ sudo apt-get upgrade**

0x1.安装 git，gdb 和 gdb-multiarch，同时安装 binfmt 用来识别文件类型

**$ sudo apt-get update**

**$ sudo apt-get install git gdb gdb-multiarch**

**$ sudo apt-get install "binfmt\*"**

0x2.安装 gdb 的插件 pwndbg

**$ git clone https://github.com/pwndbg/pwndbg**

**$ cd pwndbg**

**$ ./setup.sh**

0x3.安装pwntools

**$ apt-get install python2.7 python-pip python-dev git libssl-dev libffi-dev build-essential**

**$ pip install -U setuptools**

**$ pip install --upgrade pip**

**$ pip install --upgrade pwntools**

0x4.安装ssh

**$ sudo apt-get install ssh**

去掉22前面的#

0x5.安装ROPgadget工具

**$ pip install ropgadget**

0x6.解决了下面的问题(方法来自网上)

Traceback (most recent call last):

File "/usr/bin/pip", line 9, in <module>

from pip import main

**$ sudo gedit /usr/bin/pip**

**然后将相应的内容修改为下面的内容：**

from pip import \_\_main\_\_ //修改

if \_\_name\_\_ == '\_\_main\_\_':

sys.exit(\_\_main\_\_.\_main())//修改

0x7.安装qemu

**$ sudo apt-get install qemu-user**

0x8. 安装LibcSearcher(用处: 用来泄露libc库中函数的偏移的库)

**$ git clone https://github.com/lieanu/LibcSearcher.git**

**$ cd LibcSearcher**

**$ python setup.py develop**

0x9.安装one\_gadget(用处:用来寻找libc库中的execve('/bin/sh', NULL, NULL)可以一个gadget就可以getshell的好东西)

**$ sudo apt install ruby**

**$ gem install one\_gadget**

0xA.安装peda

**$ git clone https://github.com/longld/peda.git ~/peda**

**$ echo "source ~/peda/peda.py" >> ~/.gdbinit**

0xB.安装libcdatabase(因为安装时间太长，以后再装)

**$ cd ~**

**$ git clone https://github.com/niklasb/libc-database.git**

**$ cd libc-database**

**$ ./get**

0xC.安装32位程序依赖的环境

**$ dpkg --add-architecture i386**

**$ sudo apt-get -y install lib32z1 lib32ncurses5**

0xC.搜狗输入法 (未安装)

参考链接：

<https://www.jianshu.com/p/1476f38e3aa3>

<https://carlstar.club/2018/09/03/pwn%E7%8E%AF%E5%A2%83%E6%90%AD%E5%BB%BA/#%E5%AE%89%E8%A3%85libcdatabase>

<https://wiki.x10sec.org/>

<https://blog.csdn.net/lxlong89940101/article/details/94390393>

<https://github.com/giantbranch/pwn-env-init>