从零开始入门pwn(二):环境搭建

原创

小白之耻 于 2021-12-10 14:36:46 发布
文章标签： 安全 pwn linux 网络

目录

一.前言

前几天写了一些关于pwn的介绍以及一些前置知识，其实那些知识都是浅尝辄止就行，重点还得放在后续的做题中，边做边学不香吗，不仅有成就感还能快速熟悉pwn~~绝对不是因为没时间去专门学~~。

但是之前的前置知识主要还是为了给那些真正没有基础的小白一个相对平滑的入门曲线，对于真正想要入门pwn的同学来说，前置知识其实都已经掌握过了（不会有人真的是没一点计算机基础单纯是看pwn帅就想来入门的吧）。

所以，这就马不停蹄给已经有前置知识的同学写一个环境搭建的博客，也是分享一下目前我遇到的题目所用到的工具的分享。

二.环境搭建

一.Linux系统

上一篇博客已经说过了，绝大部分pwn题的文件都是Linux上的可执行文件，所以没有一个Linux系统的电脑完全做不了pwn。

所以把你的windows换成Linux吧。

咳咳，开个小玩笑，说到Linux系统，除了一些牛人，不会真有人放弃windows装上Linux吧，毕竟正版windows还是要钱的，所以Linux装在虚拟机上就足够用了。

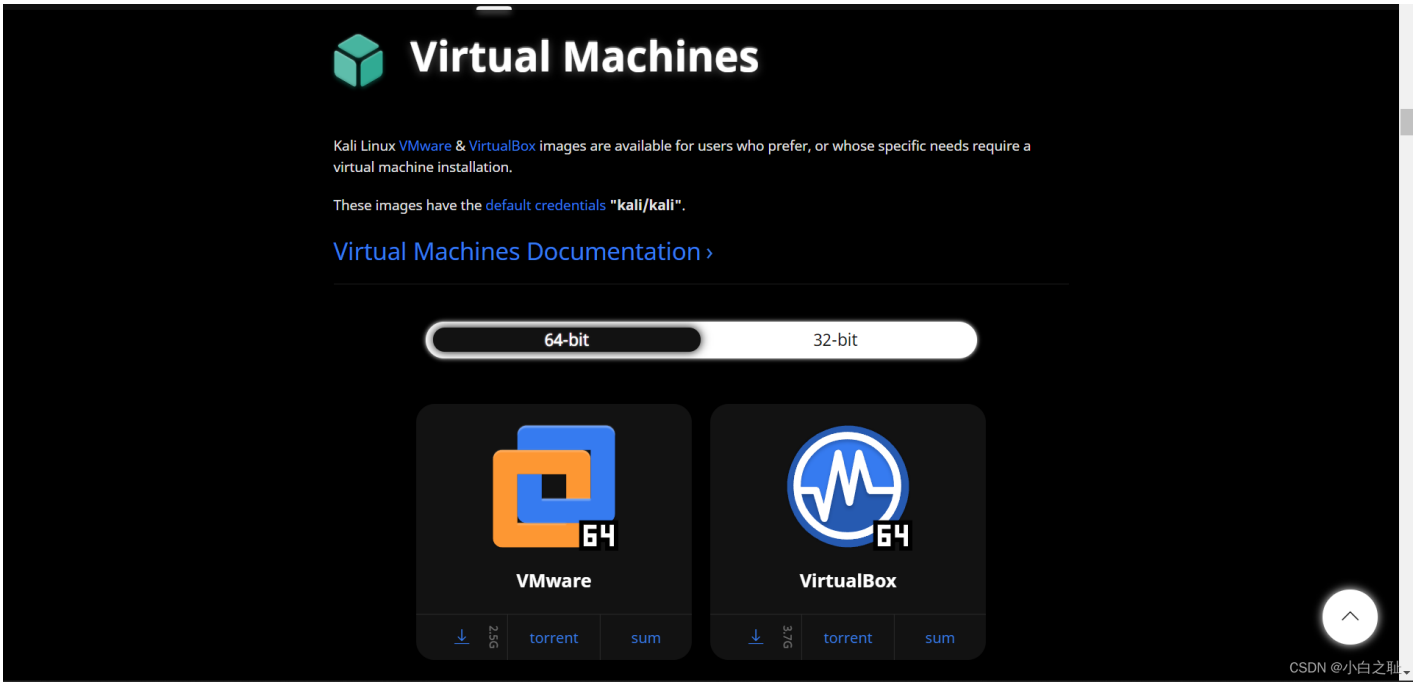
但是Linux系统这么多版本，到底要装哪一个呢，centos还是ubuntu或者奢侈一点装Redhat？

NO，对于一个CTFer来说，说到Linux就不得不提大名鼎鼎的Kali酱。

~~光看着图标就帅爆子好吗~~。在经过ubuntu和centos纯命令行的洗礼之后，我觉得kali简直就是小天使，尤其是在上面做ctf题的时候，当你觉得这个工具肯定要apt-get的时候，它偏偏会给你惊喜，几乎CTFer所需要的所有工具都被包含在这个小天使里面，几乎是随叫随到，而且干净整洁的图形界面让人心旷神怡。

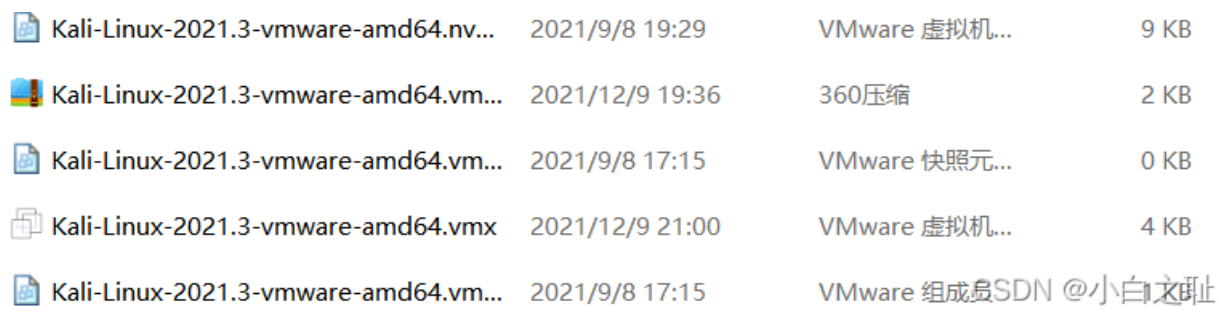
贴心的kali官网也是给你打包好了你想要的一切，直接把东西下载下来解压双击，直接把虚拟机安排上

下载网址： Get Kali | Kali Linux



进入下载网址后选择你所用的虚拟机软件，VMware或者Virtualbox，点击下载（话说为什么virtualbox的大这么多啊）

由于我用的是VMware，所以这里用VM的做演示，下载好的压缩包解压在一个文件夹。~~除非你想你的数据是一次性的~~



可以看到解压后有一个vmx文件（图中第四个），直接点开，直接开机，完事！**PS:开机用户和密码都是kali**

至于要不要汉化嘛，看你自己的意愿了

(48条消息) kali汉化_玄予的博客-CSDN博客_kali汉化包

二.pwntools

安装完虚拟机，就可以开始pwn的工具的准备了，pwntools顾名思义，就是pwn的工具们。

pwntools是一个python的库，里面集合了各种各样有关于pwn的函数，在我们写脚本攻破文件的时候基本工具就是pwntools，而pwntools的安装方式也很简单，官网也写得很清楚，但是我猜你们懒得去官网找，所以就把代码搬上来

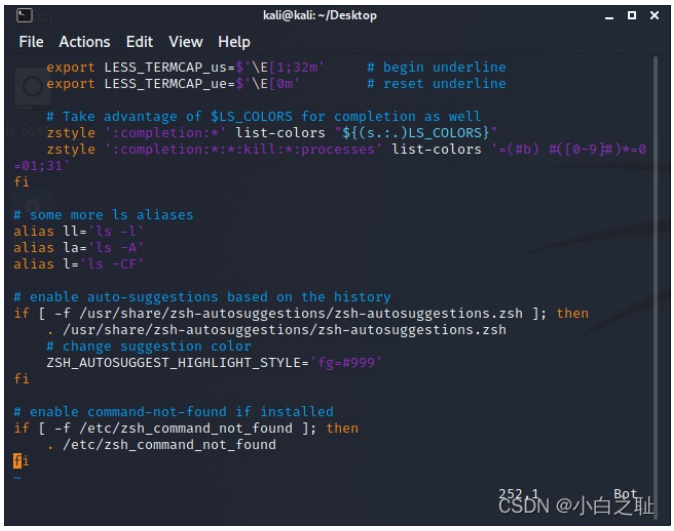
打开kali酱的控制台，复制代码，粘贴，回车，搞定，但是根据官网的指令做可能会有一点警告，虽然无伤大雅，但是看着总是不舒服。

```
sudo apt-get update
sudo apt-get install python3 python3-pip python3-dev git libssl-dev libffi-dev build-essential
```

究其原因还是因为环境变量的问题，先输入以上代码之后再进行以下操作

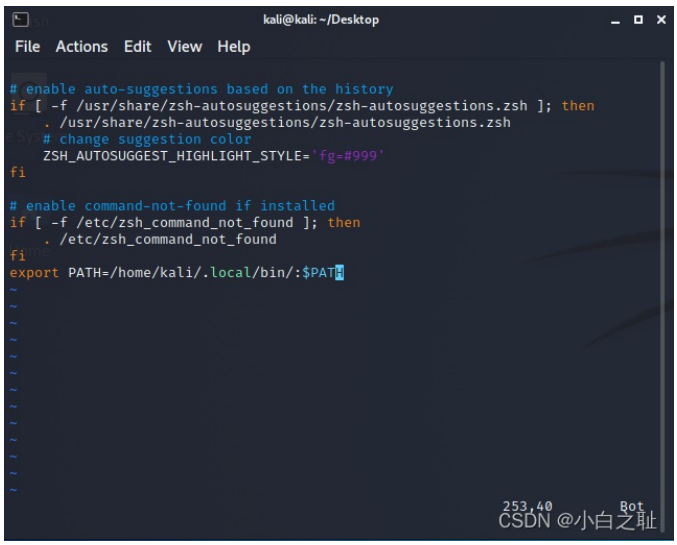
```
vim ~/.zshrc
```

Shift+g跳到最后



按o新加一行，并输入以下字符

```
export PATH=/home/kali/.local/bin/:$PATH
```



esc后:wq保存(这属于是把奶喂嘴里了)

最后输入以下代码，完事

```
source ~/.zshrc
python3 -m pip install --upgrade pip
python3 -m pip install --upgrade pwntools
```

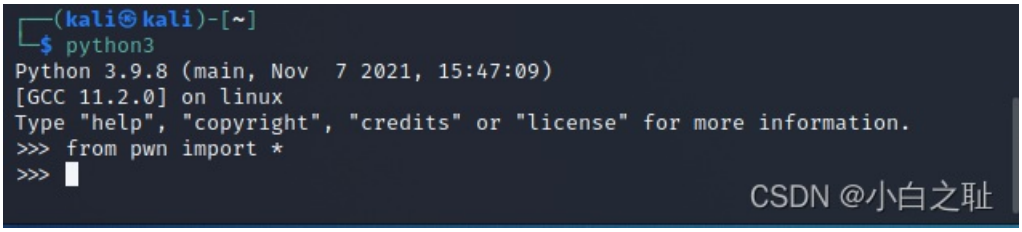
注意，这里是安装python3的代码，如果要使用python2

```
apt-get update
apt-get install python python-pip python-dev git libssl-dev libffi-dev build-essential
python2 -m pip install --upgrade pip==20.3.4
python2 -m pip install --upgrade pwntools
```

不过python2好像已经停止更新了，所以我还是推荐用python3，记住以后要用这个库都要用python3命令哦。

kali酱已经自带了python2和python3，就不用自己安装python了，kali yyds！

安装完成后，在控制台输入python3进入python3命令模式，输入from pwn import *



如果没有报错，说明安装成功

三.pwngdb

pwn题中二进制文件几乎都是要首先在自己的机子上跑，同时你要在自己的机子上面攻击掉了这个文件你才有可能攻击掉赛方的文件。所以我们要做出pwn题的第一件事，就是获取自己的电脑控制权(bushi)。而pwn掉自己的电脑，就需要用到调试。

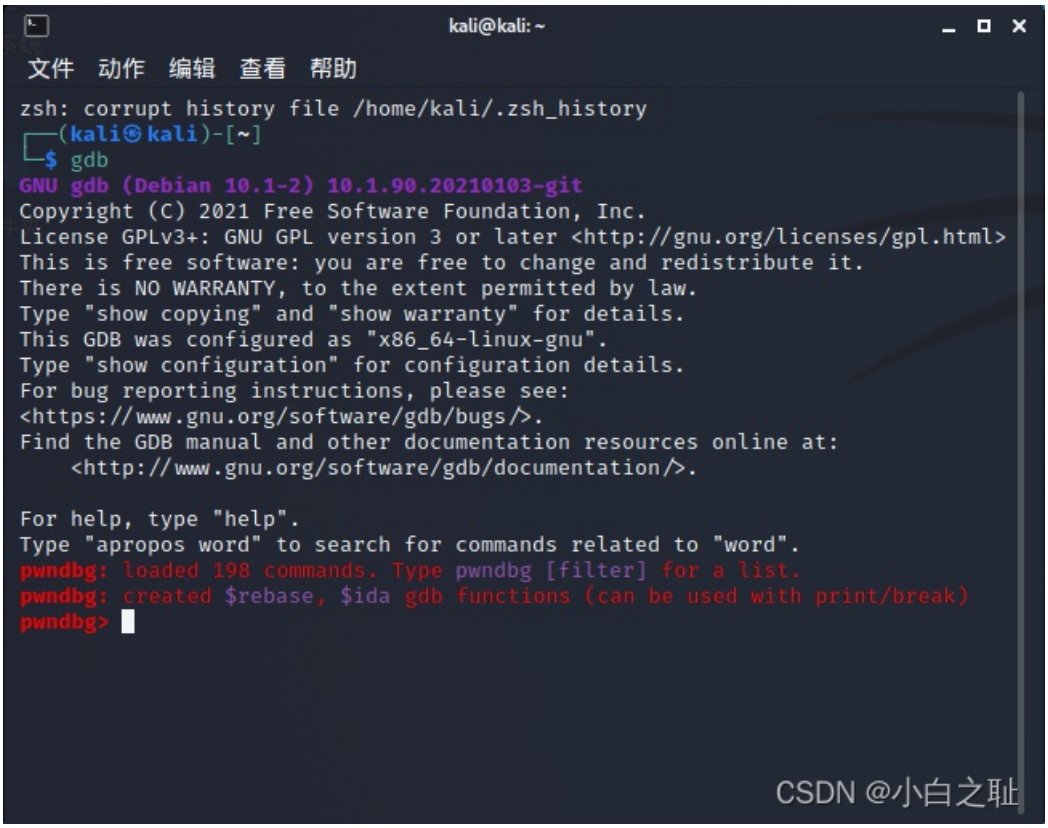
俗话说的好，**静态调试看IDA，动态调试看pwngdb**（其实动态调试也能用IDA啦），pwngdb可以帮助你在可执行文件**执行的时候**查看各种寄存器的值，以及函数地址和偏移量，甚至可以让你一条汇编语言一条汇编语言分析，是分析程序不可或缺的工具。

安装指令

```
git clone https://github.com/pwndbg/pwndbg
cd pwndbg
./setup.sh
```

记得要在/home/kali下面的控制台执行这几条指令，除非你更改了里面的安装位置，否则安装完之后pwndbg文件夹也不要移动

执行完这几条指令后在控制台输入gdb



当看到以上画面时说明安装成功。

四.IDA

~~IDA为什么是神~~

IDA是一个非常牛逼的反编译工具，可以把可执行文件反编译成汇编语言来让我们攻破阅读，同时IDA自带的插件可以帮助我们把汇编语言转化成C语言形式，帮助我们更好地分析程序，这也是为什么上一篇博客需要大家学习C语言的原因，但是程序最终还是要归约到地址上，IDA也将这些地址相应的指令反汇编出来，可以说即使是初学者，也能够很容易通过IDA分析出栈的位置。

而且IDA还自带着动态调试的功能，前提是需要将在linux上运行，用远程linux运行也可以，如果实在看不懂gdb也可以直接用IDA动态调试，具体操作在后续博客中会详细说明

但是，IDA pro是付费的

如果有能力的同学可以自行购买正版

IDA Pro – Hex Rays (hex-rays.com)

官网就放这里了

[redacted]

五.大脑&时间

虽说有了工具，但是就算是计算机，有了键盘屏幕也要一个好的、活跃的CPU，CTFer更不例外，工具始终只是帮助我们做出题目，真正如何做出题目还是要我们有一个善于思考、用于钻研的大脑，本人虽然入门pwn也不久，但是也深深感受到真正理解一道没看过的pwn题的困难，就算把大佬的writeup给我，要看懂也是一件不容易的事。需要我们付出大量的时间和脑力来思考和理解。

所以如果真心想入门pwn，准备好你的时间和大脑，pwn掉自己的电脑吧(笑)

三.总结

本文列出了我目前遇到的题目用到的工具，后续如果有题目需要其他的工具，我会在以后的博客中更新。

这些工具大都需要上一篇博客中提到的前置知识来使用，所以希望没有相应知识的同学先去学习好前置的知识再来配置环境，免得有工具心痒痒。注意，**浅尝辄止**。

这些工具的使用我会在后续的博客中陆续更新，不过其实这些工具我也不算是特别会用，只是把我使用的经验写出来，大家如果想看的话就期待吧，当然大佬就随便看看啦。

如果你已经看完了这篇博客并且配置好了这些环境，那你就是pwn的人了，也是开始真正踏入pwn的世界了，可以开始帅气的黑客之路了。

既然都看到这里了，还不给个赞吗，跟着我一起进步，~~一起从入门到入狱~~。