逆向工程入门：IDAwindows本地动态调试，linux远程动态调试及虚拟机配置

原创

June_gjy 于 2021-02-11 09:50:29 发布 595 收藏 2

分类专栏： 网络安全 文章标签： ubuntu linux vmware 安全

本文链接：https://blog.csdn.net/weixin_50549897/article/details/113772269

本人水平有限，有不当之处欢迎指出

文章目录

一、虚拟机配置

VMware虚拟机是主流的虚拟机之一。我主要讲VMware Workstation Pro虚拟机的创建。首先从官网上下载VMware Workstation Pro。

官网链接

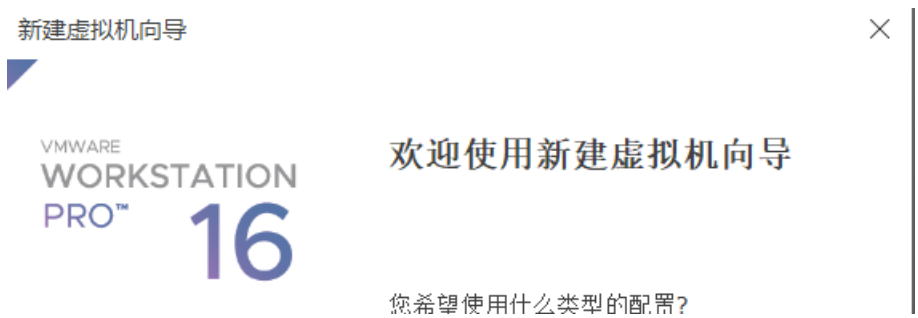
从各种渠道获取密钥后可以开始使用。

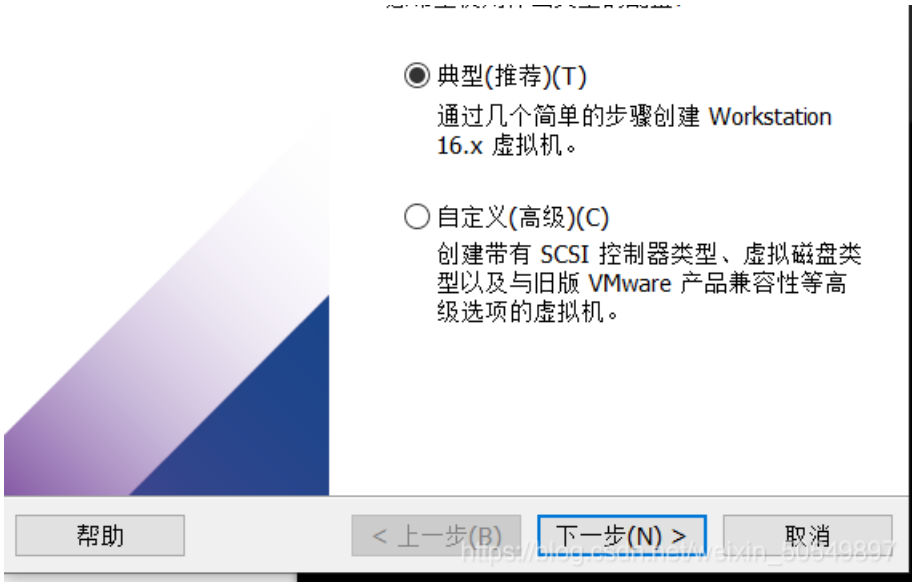
接着从ubuntu官网下载64位或32位的linux操作系统镜像

ubuntu官网

（tips：从网上其它渠道下载可能速度会更快）

打开VMware，再文件里选择新建虚拟机



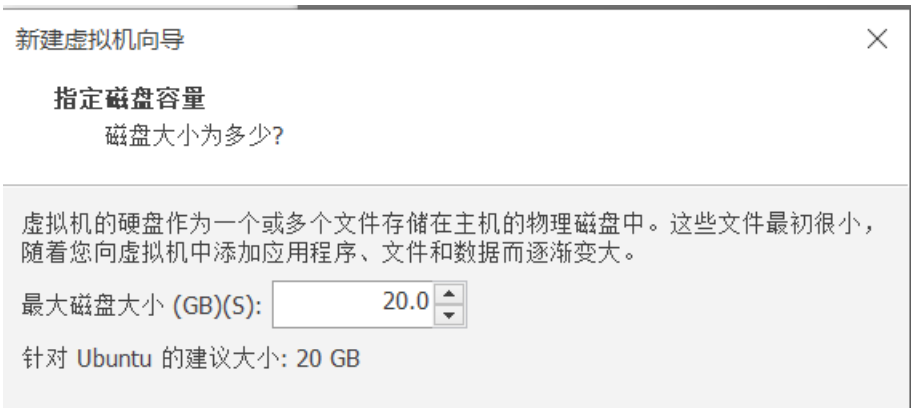


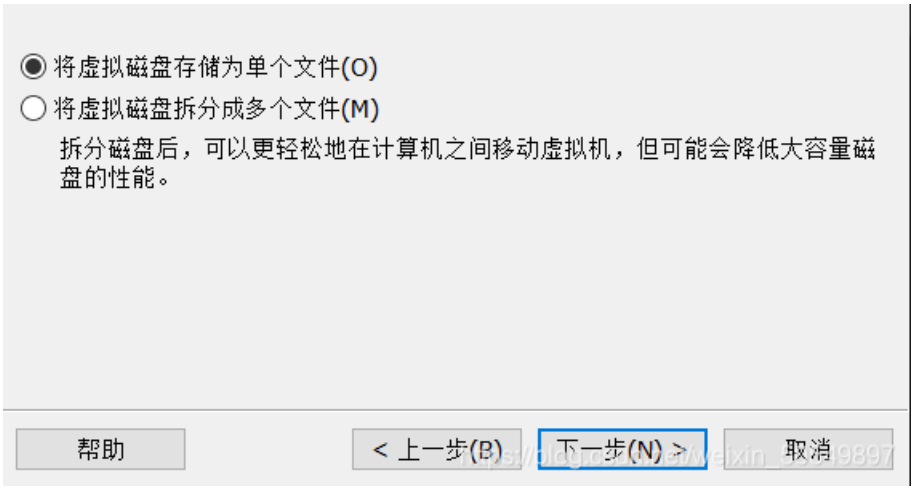
在选择安装镜像光盘文件里选择你要安装的操作系统的镜像文件

- [

下一步命名设置密码等等

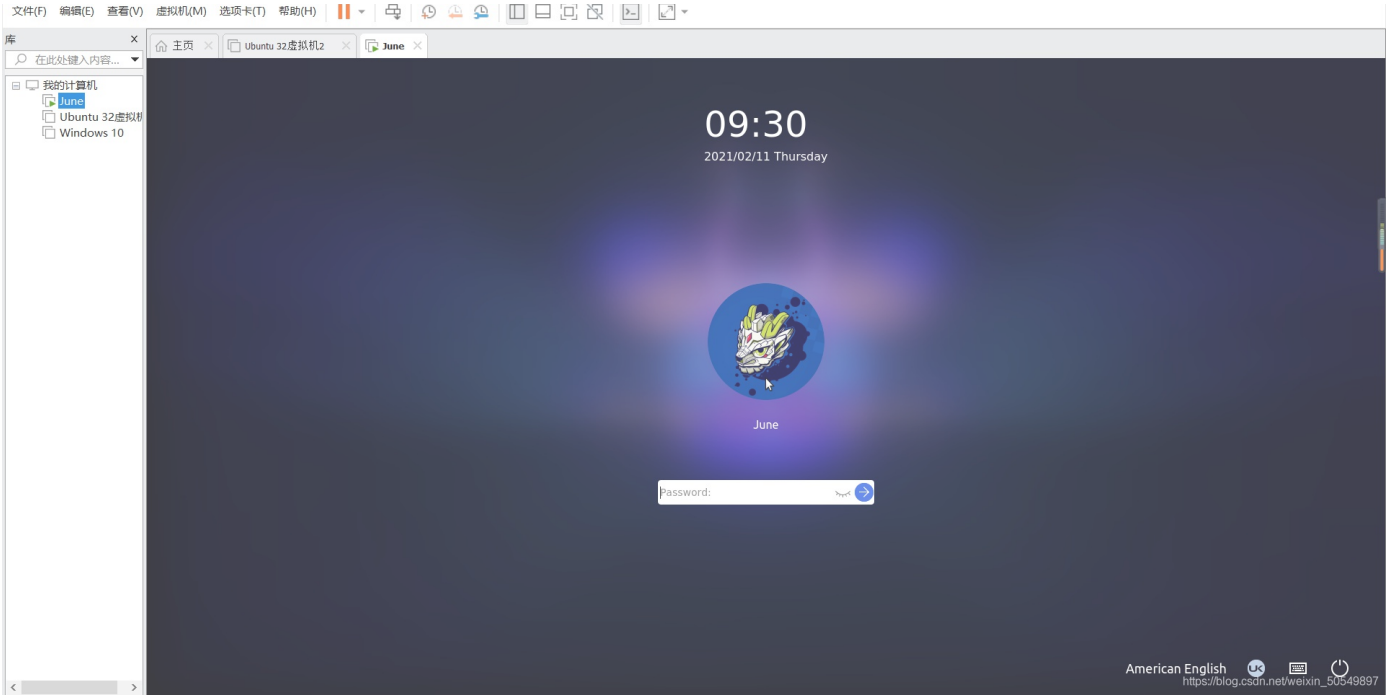
-





然后设置磁盘大小，建议选择将虚拟磁盘储存位单个文件。

设置好后，创建成功即可开机。

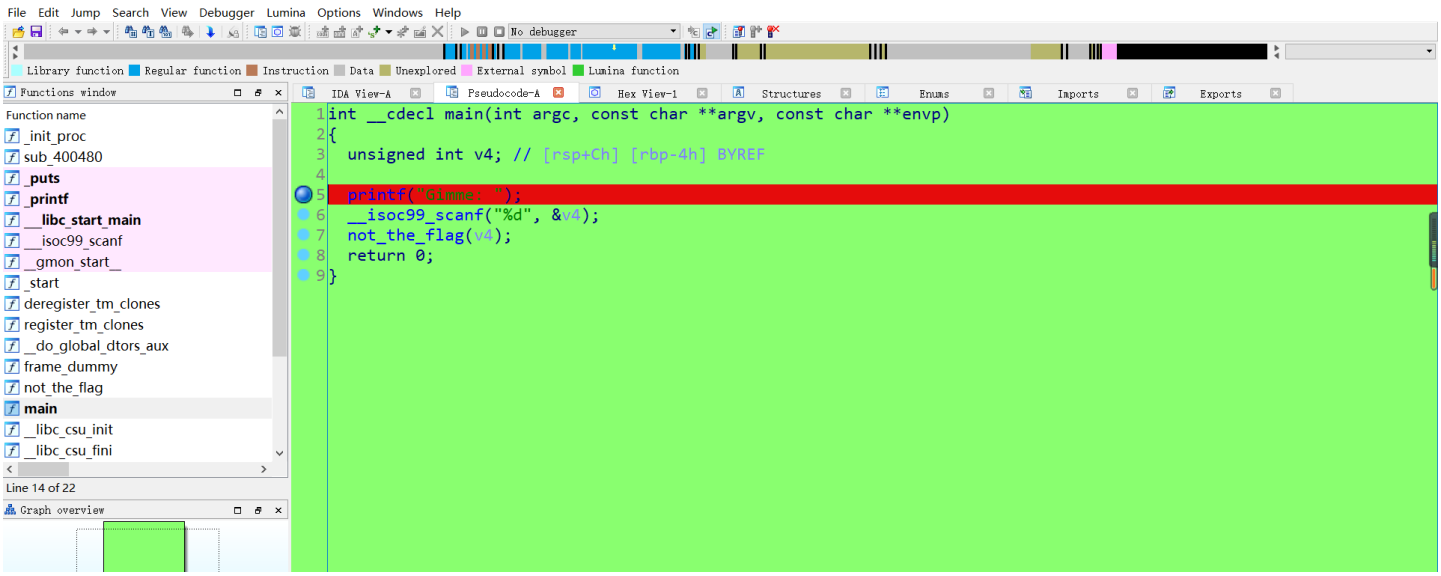


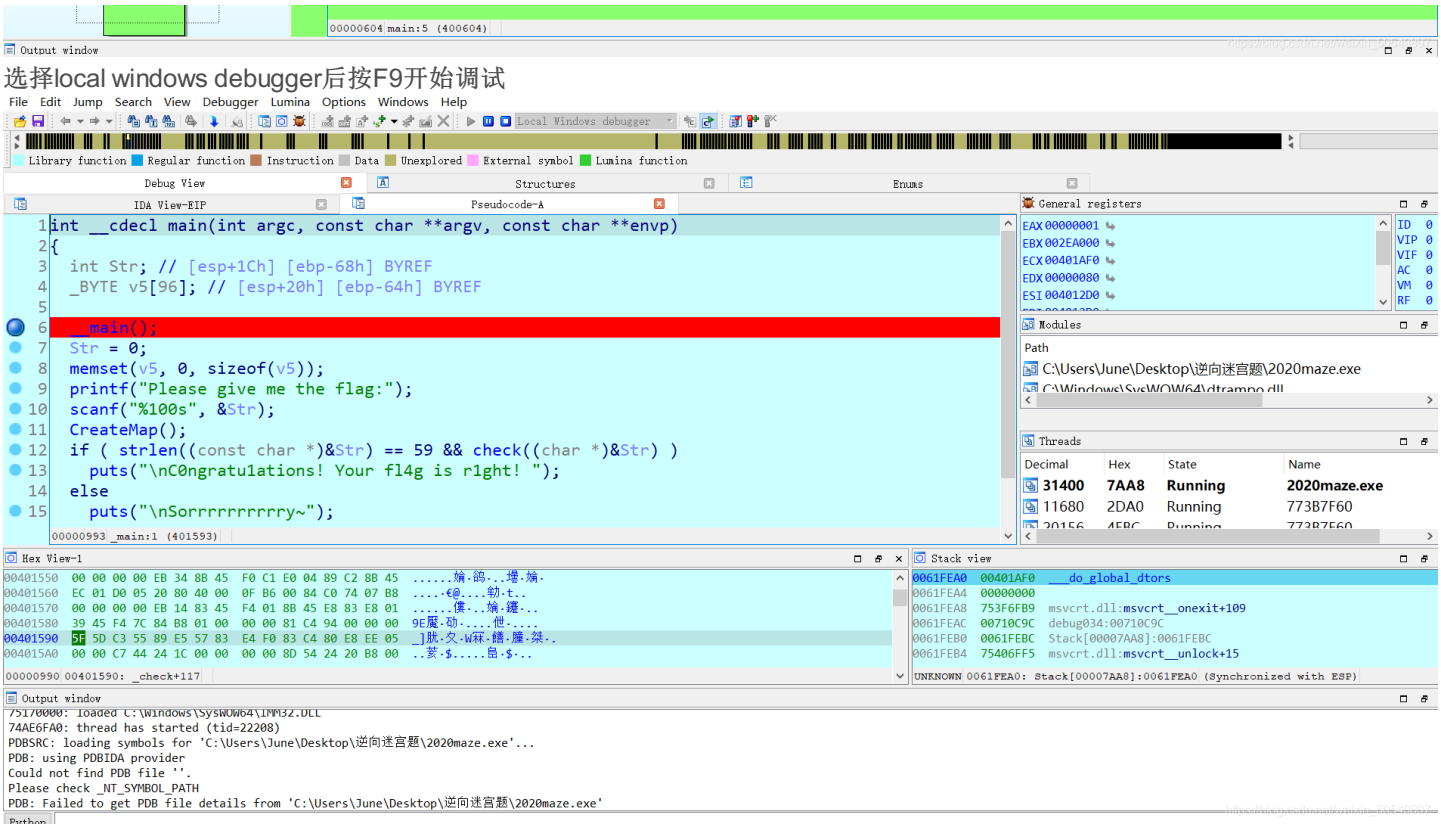
二，IDA动态调试

1.windows本地调试

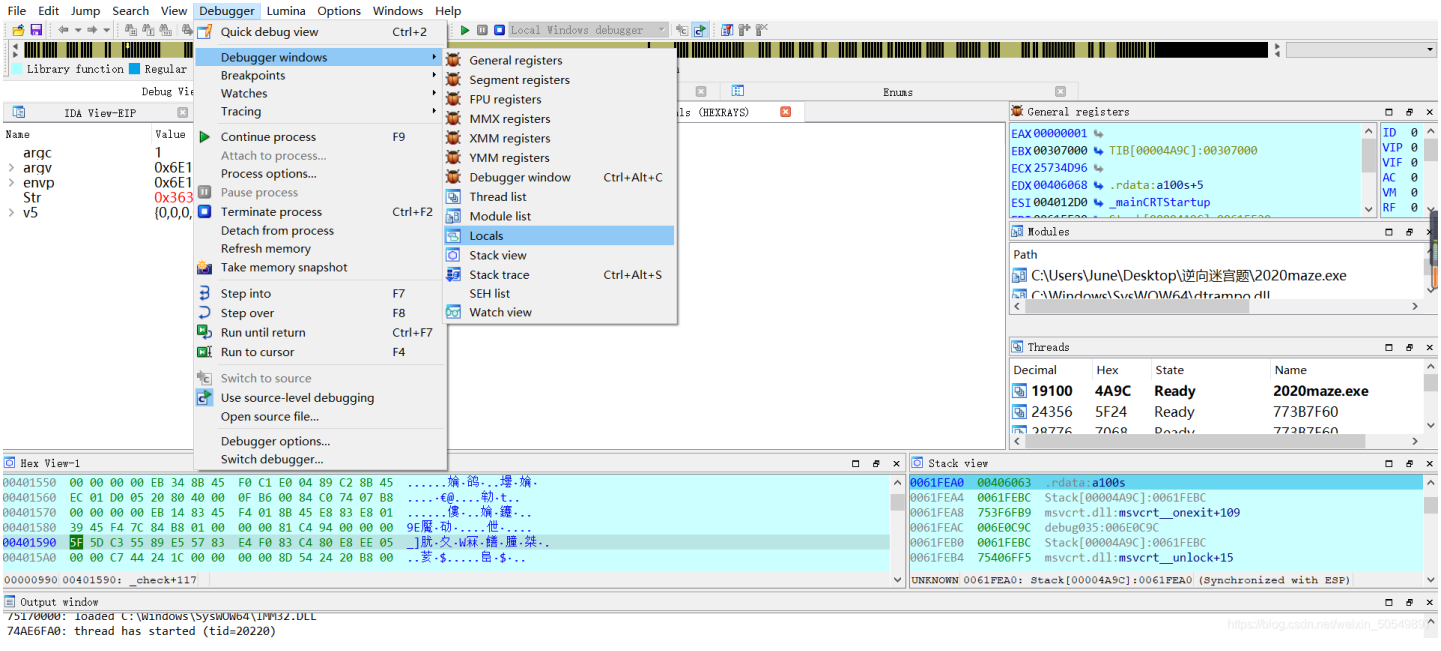
尽量使用IDA7.5进行调试，以下版本可能有bug

首先设置断点





按F8向下一条一条执行，在debugger—debugger windows—locals窗口里可以查看变量的值和相应的地址。

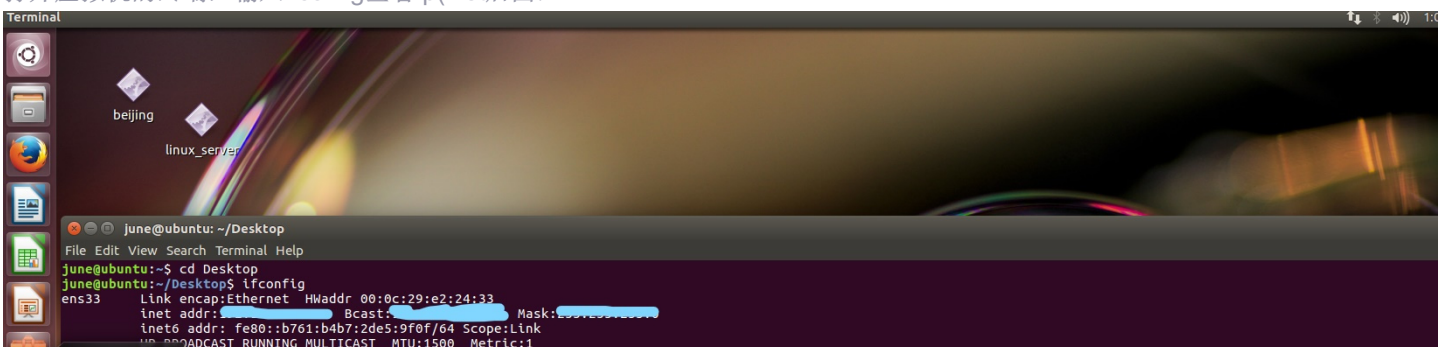


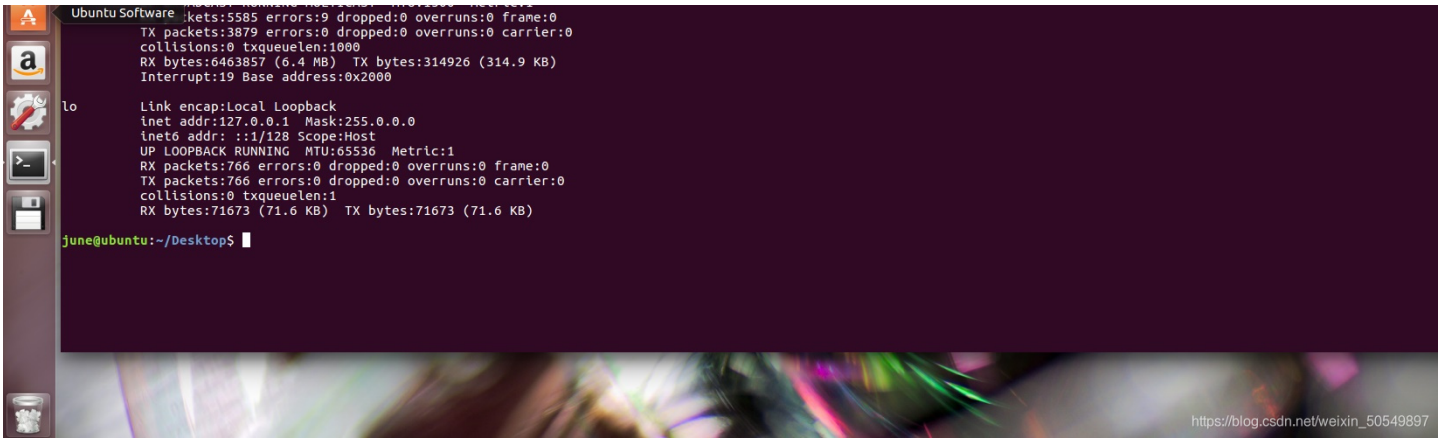
2.linux远程调试

首先打开IDA的dbgsrv复制里面的linux_server(对应32位）或linux_server64（对应64位），黏贴到对应的linux虚拟机。并且将需要调试的文件也复制过去。

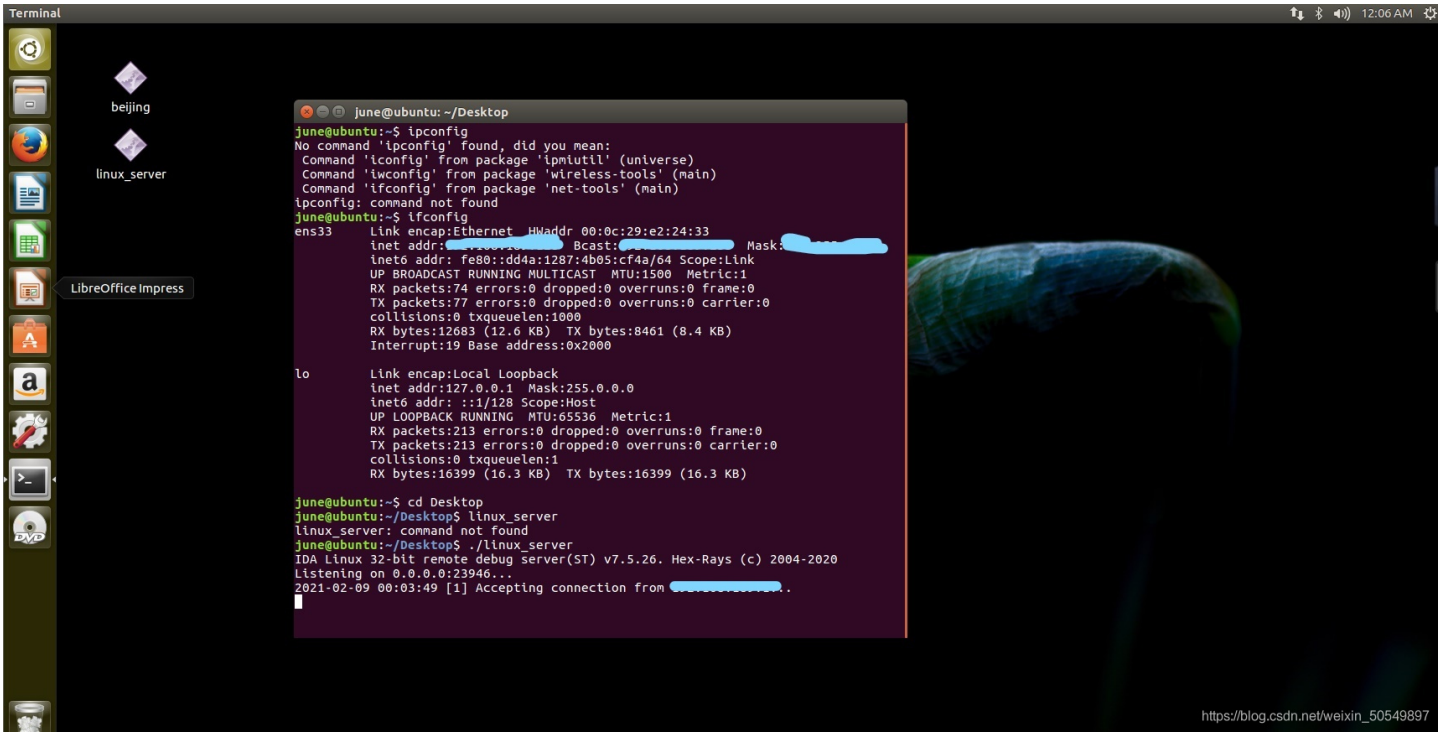
我以一个32位的ELF文件为例。

打开虚拟机的终端，输入ifconfig查看ip(inet后面）

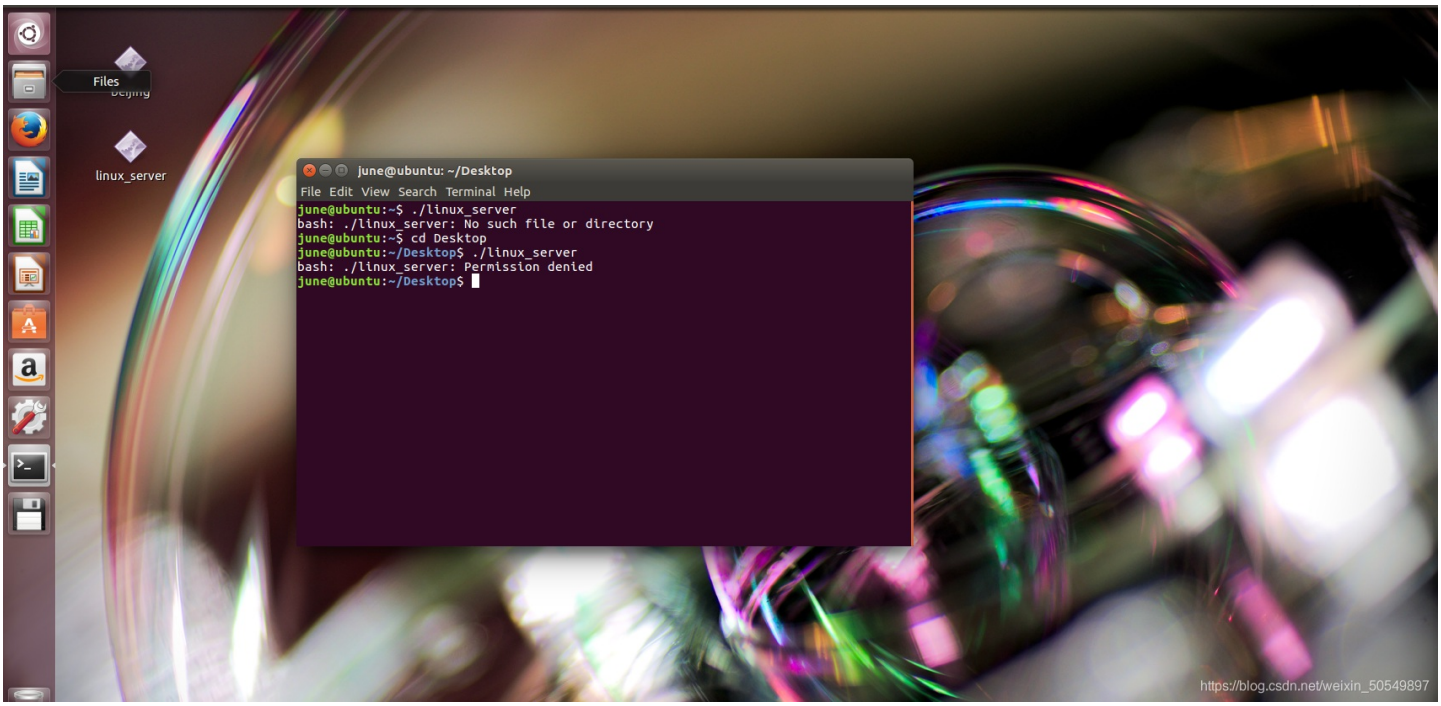




接下来cd 到linux_server的目录（我这里是Desktop）输入./linux_server启动,可以看到正在监听23946端口



如果出现以下情况表明没有权限

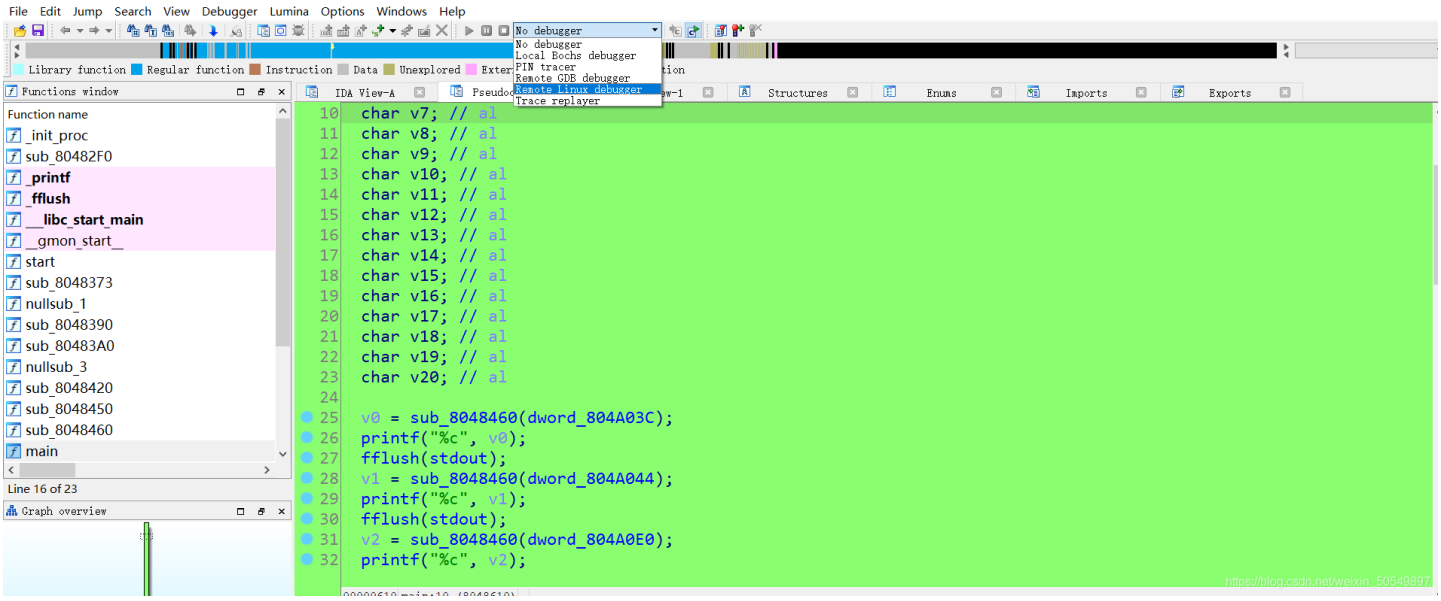


需要输入以下命令给权限

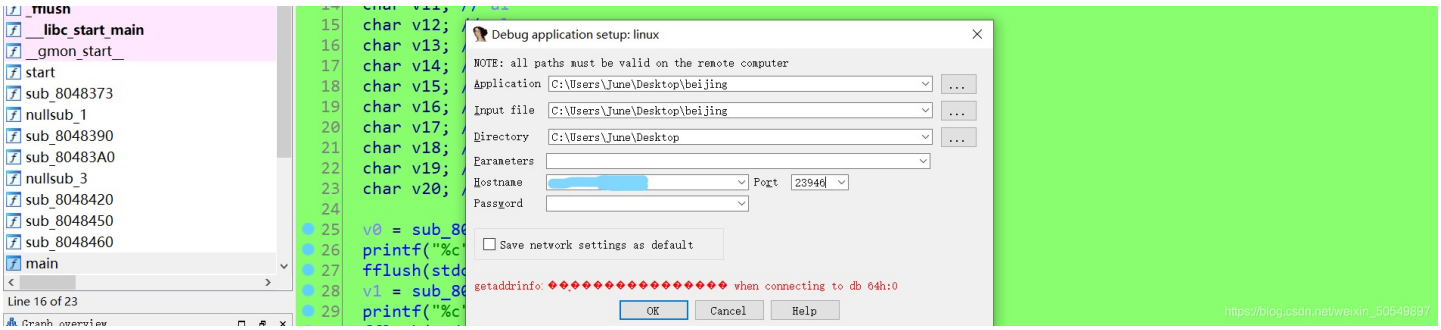
```
chmod 777 ./linux_server
```

然后在IDA的调试选...

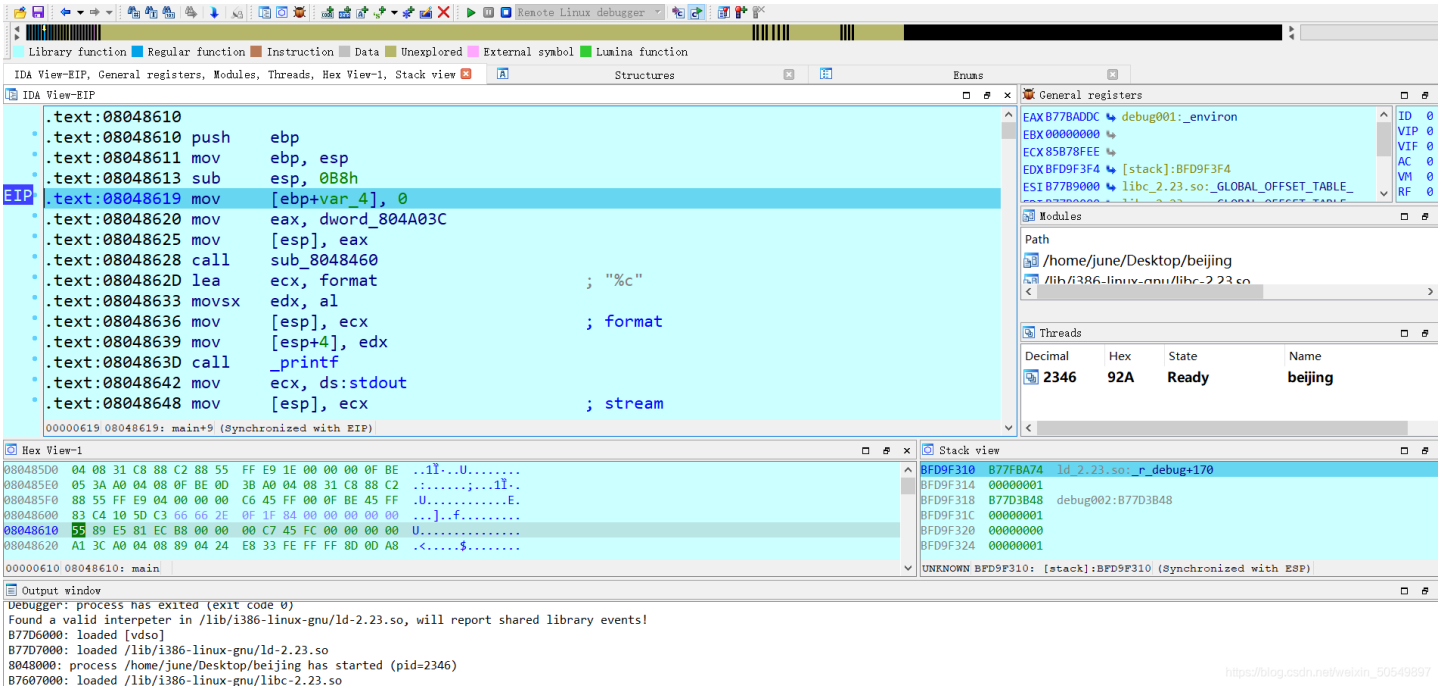
然后在IDA的调试选remote linux debugger,按F9.



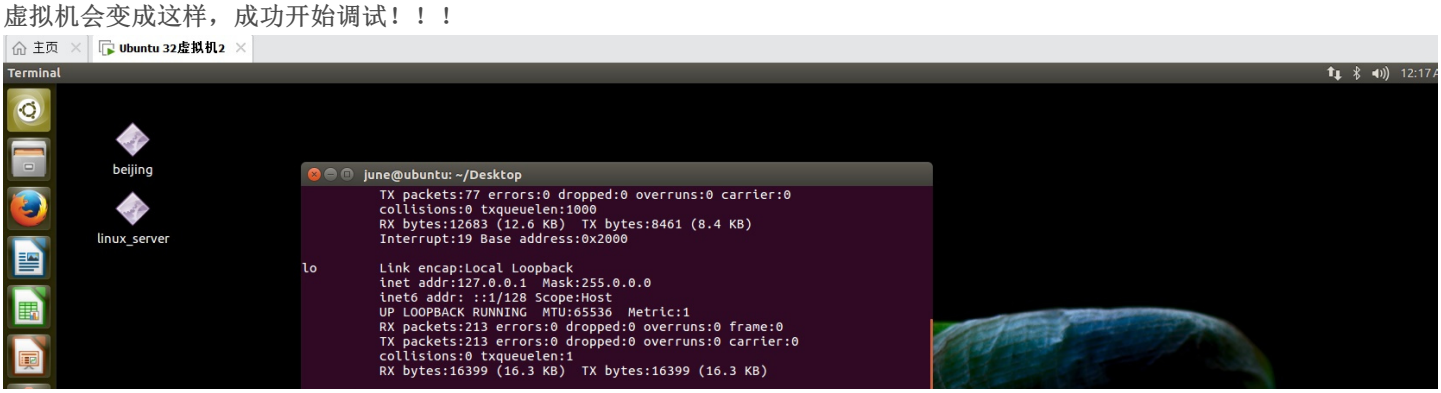
出现以下界面

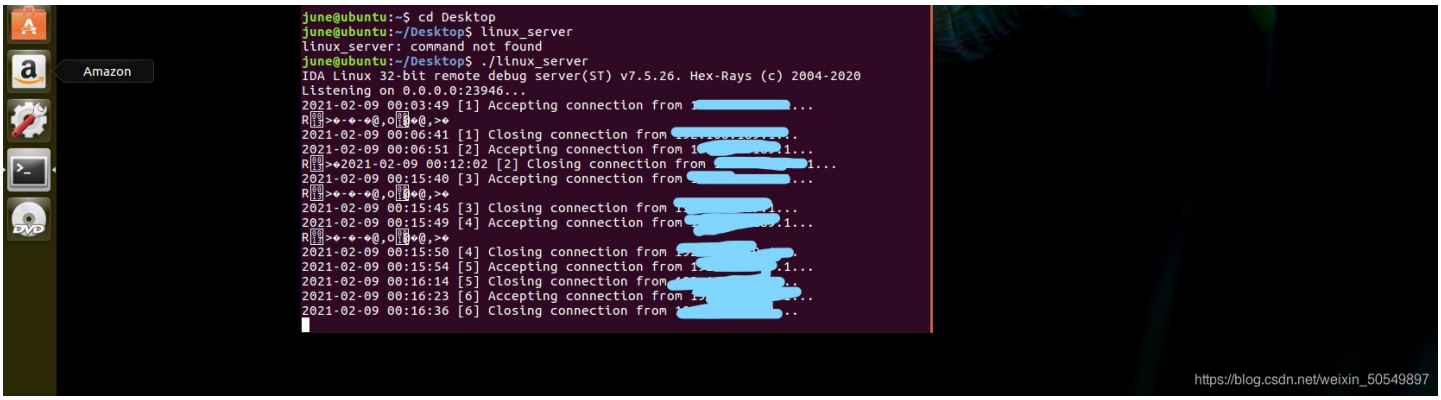


在Hostname里填上虚拟机的ip,端口填上对应的端口，确定后开始调试



虚拟机会变成这样，成功开始调试！！！





如果IDA显示无法连上虚拟机则需要关闭防火墙或重置虚拟网卡。

关闭防火墙：先输入以下,然后输入三次原密码

```
sudo passwd
```

再输入

```
su root
```

接着输入以下命令关闭防火墙

```
ufw disable
```

若还不行则重置虚拟网卡，见以下这篇文章

https://www.jianshu.com/p/d70622414101

本人其它文章链接

逆向迷宫题总结（以四道题目为例）

BUUCTF reverse：[GXYCTF2019]luck_guy,findit,简单注册器题解

封神台靶场尤里的复仇I第一第二第五第六第七章解题思路(持续更新）

ctfhub:网鼎杯第一场2018 reverse-beijing题解