# 第二次作业

1.关于固件解包

从网上下载固件，链接如下：

<ftp://ftp2.dlink.com/PRODUCTS/DIR-815/REVA/DIR-815_FIRMWARE_1.01.ZIP>

安装binwalk：

$ sudo apt-get update

$ sudo apt-get install build-essential autoconf git

# https://github.com/devttys0/binwalk/wiki/Quick-Start-Guide

$ wget https://github.com/devttys0/binwalk/archive/master.zip

$ unzip master.zip

$ (cd binwalk-master && sudo python setup.py uninstall && sudo python setup.py install)

# 自动安装依赖库文件和工具组件

$ sudo ./binwalk-master/deps.sh

$ sudo apt-get update

$ sudo apt-get install build-essential autoconf git

# https://github.com/devttys0/binwalk/blob/master/INSTALL.md

$ git clone https://github.com/devttys0/binwalk.git

$ cd binwalk

# python2.7安装

$ sudo python setup.py install

# python2.7手动安装依赖库

$ sudo apt-get install python-lzma

$ sudo apt-get install python-crypto

$ sudo apt-get install libqt4-opengl python-opengl python-qt4 python-qt4-gl python-numpy python-scipy python-pip

$ sudo pip install pyqtgraph

$ sudo apt-get install python-pip

$ sudo pip install capstone

# Install standard extraction utilities（必选）

$ sudo apt-get install mtd-utils gzip bzip2 tar arj lhasa p7zip p7zip-full cabextract cramfsprogs cramfsswap squashfs-tools

# Install sasquatch to extract non-standard SquashFS images（必选）

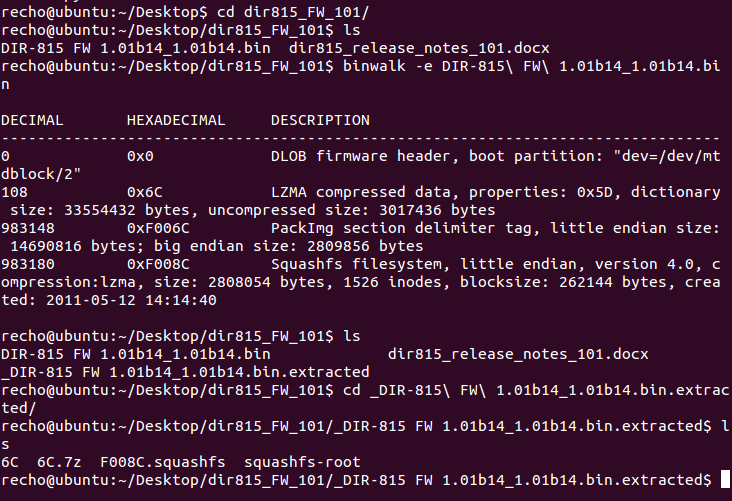
$ sudo apt-get install zlib1g-dev liblzma-dev liblzo2-dev $ git clone https://github.com/devttys0/sasquatch

$ (cd sasquatch && ./build.sh)注：解压文件系统的文件下载的时候网站可能不可信赖，这个时候打开build.sh文件把里面那条wget命令后面加上--no-check-certificate再加网址即可

安装链接:

<https://blog.csdn.net/QQ1084283172/article/details/65441110?utm_source=blogxgwz1>

固件解包如下：



2.环境搭建

参考链接:<http://www.10tiao.com/html/523/201608/2458279448/3.html>

安装qemu:

git clone git://git.qemu.org/qemu.git

cd qemu

git submodule init

git submodule update --recursive

apt install libglib2.0 libglib2.0-dev

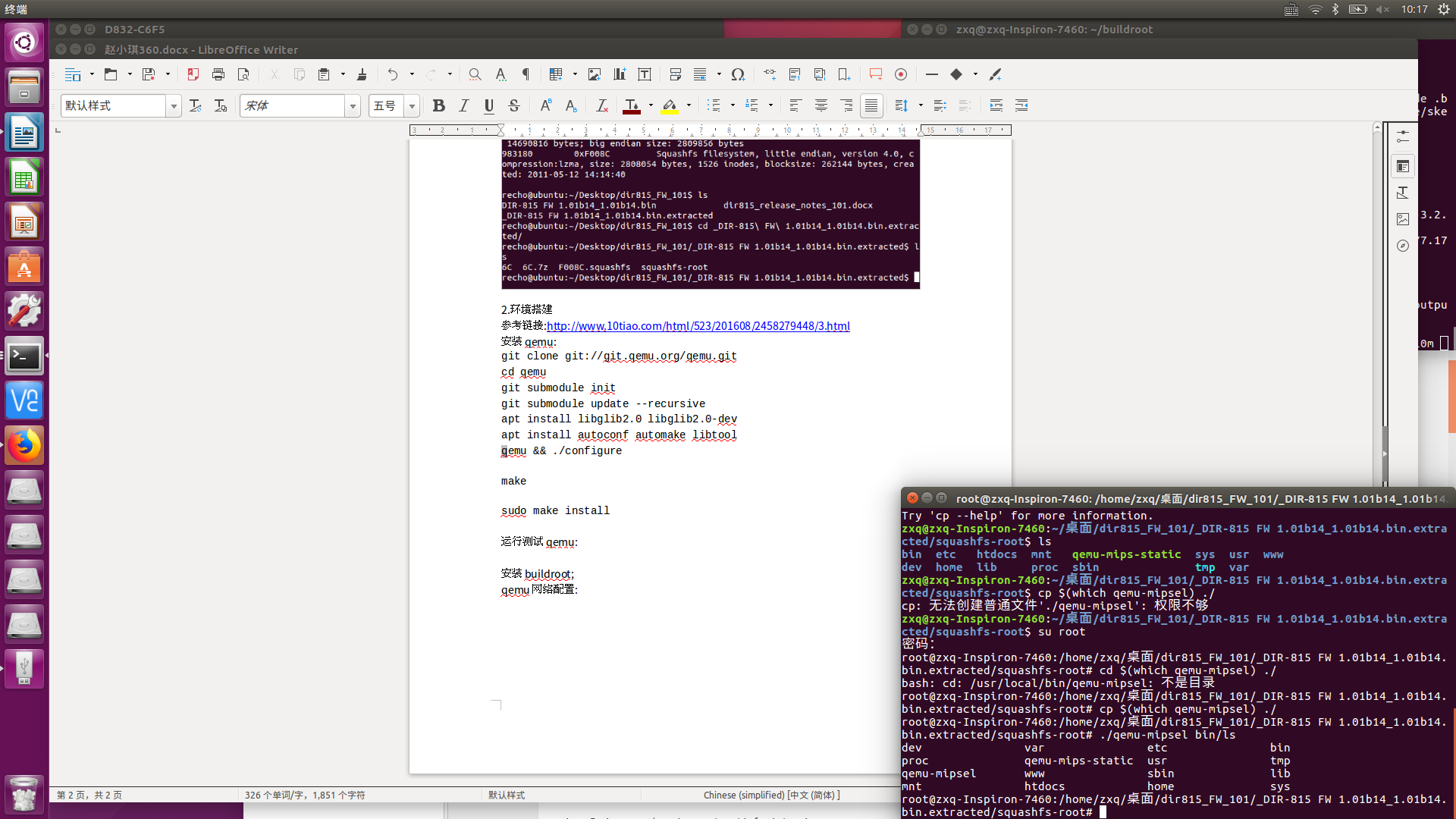
apt install autoconf automake libtool

qemu && ./configure

make

sudo make install

运行测试qemu:



安装buildroot;

编译编写存在漏洞的mips可执行文件及编写mips可用的shellcode，故需要在linux上搭建交叉编译环境。

wget <http://buildroot.uclibc.org/downloads/snapshots/buildroot-snapshot.tar.bz2>

tar -jxvf buildroot-snapshot.tar.bz2

完成下载及解压后，执行如下命令。

cd buildroot

sudo apt-get install libncurses5-dev patch

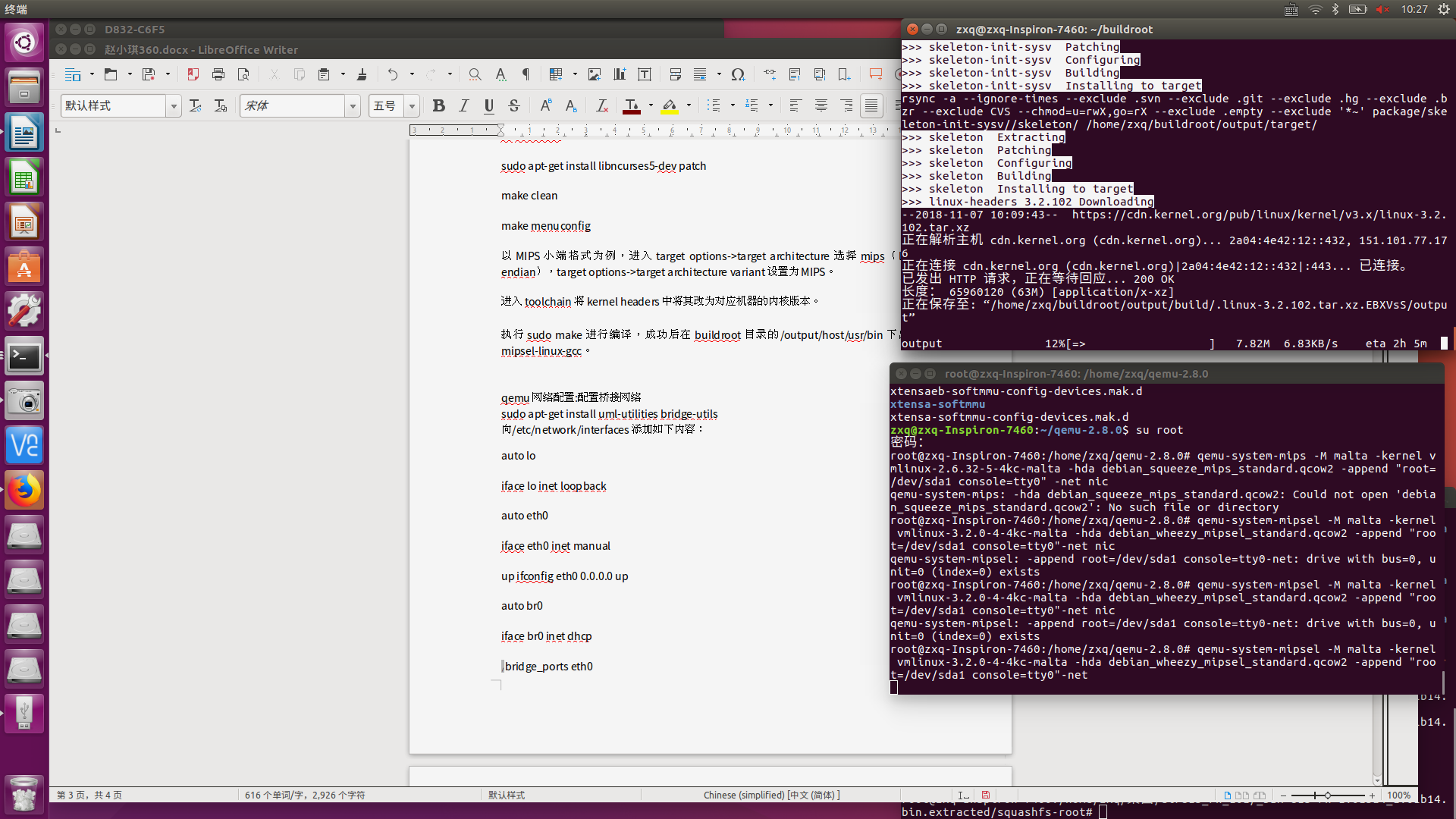
make clean

make menuconfig

以MIPS小端格式为例，进入target options->target architecture选择mips（little endian），target options->target architecture variant设置为MIPS。

进入toolchain将kernel headers中将其改为对应机器的内核版本。

执行sudo make进行编译，成功后在buildroot目录的/output/host/usr/bin下出现mipsel-linux-gcc。



qemu网络配置:配置桥接网络

sudo apt-get install uml-utilities bridge-utils

向/etc/network/interfaces添加如下内容：

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet manual

up ifconfig eth0 0.0.0.0 up

auto br0

iface br0 inet dhcp

​ bridge\_ports eth0

​ bridge\_stp off

​ bridge\_maxwait 1

在/etc/qemu-ifup中写入如下内容：

#!/bin/sh

echo "executing /etc/qemu-ifup"

echo "bringing up $1 for bridged mode..."

sudo /sbin/ifconfig $1 0.0.0.0 promisc up

echo "adding $1 to br0..."

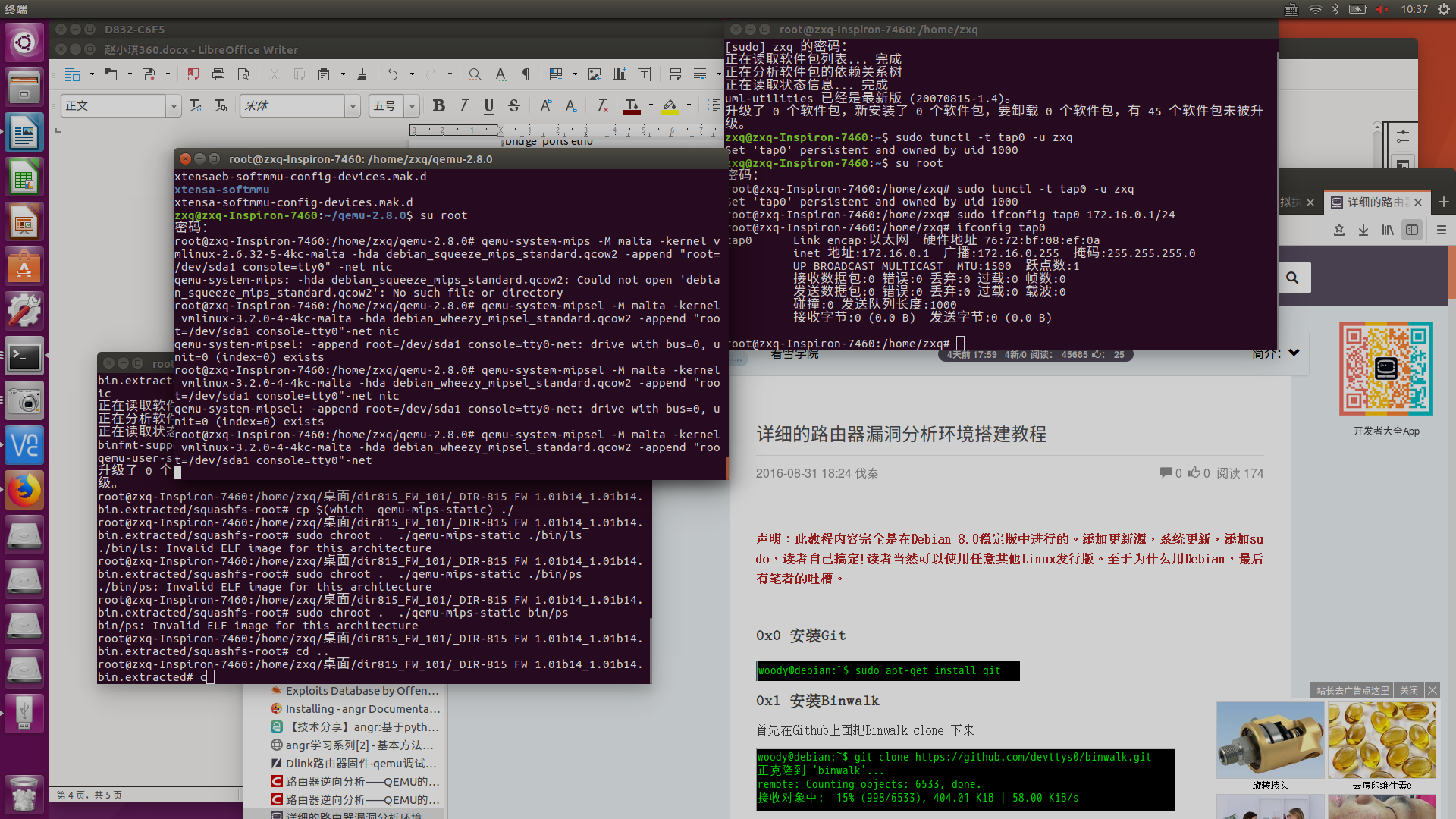
sudo /sbin/brctl addif br0 $1

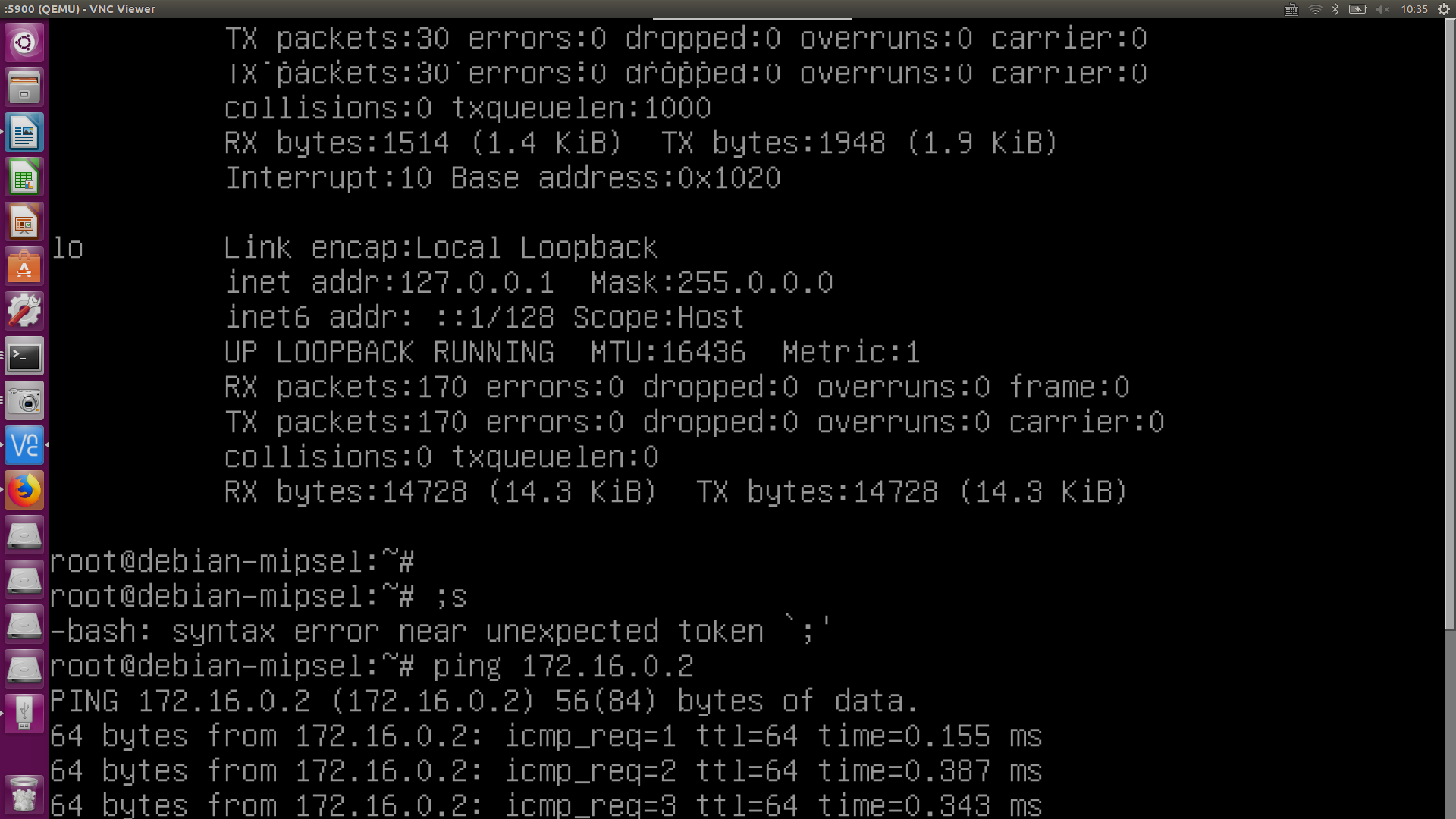
sleep 2

保存退出后使用chmod a+x为其加上可执行属性。输入sudo service networking restart重启网络使设置生效。sudo ifdown eth0&sudo ifup br0。

下载内核文件和磁盘镜像并安装:

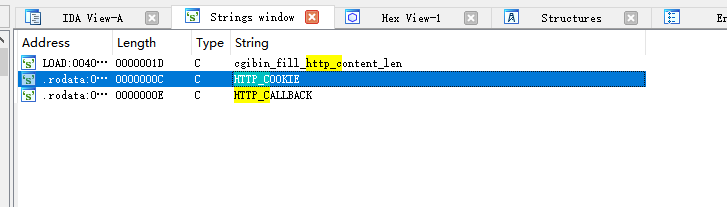
https://people.debian.org/~aurel32/qemu/mips/



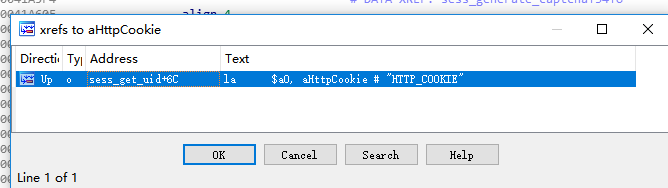


1. 漏洞分析

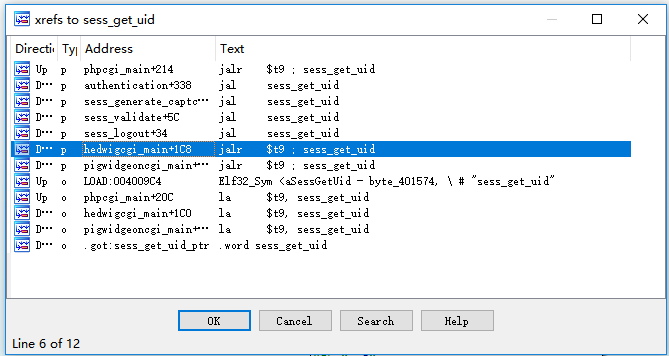
将固件中的cgibin放入ida中进行分析，漏洞出现在Hedwig.cgi中快速定位字符串，快速定位字符串



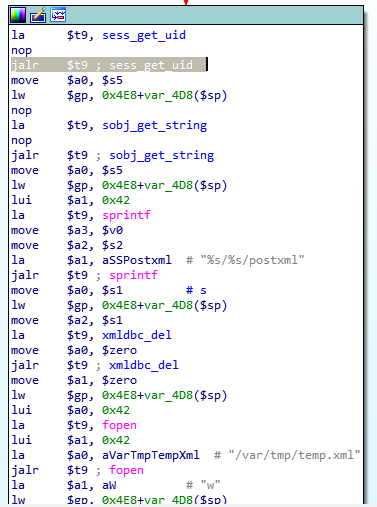
查看交叉引用信息



查看该函数的交叉引用信息



跳到此处查看该函数



观察到后面有个危险的函数sprintf，也就是说如果cookie的长度过长可能造成溢出。

动态调试验证不太会用。。。。。。