Dlink路由器固件-qemu调试环境搭建

sebao / 2017-09-26 07:56:00 / 浏览数 7132

简介：

QEMU是一套由法布里斯·贝拉(Fabrice
Bellard)所编写的以GPL许可证分发源码的模拟处理器，在GNU/Linux平台上使用广泛。Bochs，PearPC等与其类似，但不具备其许多特性，比如高速度及跨平台的特性，

qemu和vmware一样，一种虚拟机软件，只不过qemu能够虚拟的平台更加丰富一些。能够虚拟很多嵌入式平台的设备。

在qemu我们可以运行路由器固件，进行调试，以及漏洞挖掘。大大减少研究成本。穷人必备技能。

固件下载

从官网 ftp://ftp2.dlink.com/PRODUCTS/ 下载路由器固件，然后用binwalk解开固件。

binwalk安装

解路由器固件需要用到binwalk。

本人建议下载源码，自己编译安装，这样可以安装到最新版本，还有一个原因就是 apt-get安装的binwalk会缺少很多依赖。

```
$ 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■■
$ sudo python setup.py install

# python2.7■■■■■■■
$ 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■■■■
$ 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■■■■
$ sudo apt-get install zlib1g-dev liblzma-dev liblzo2-dev
$ git clone https://github.com/devttys0/sasquatch
$ (cd sasquatch && ./build.sh)

# Install jefferson to extract JFFS2 file systems■■■■
$ sudo pip install cstruct
$ git clone https://github.com/sviehb/jefferson
$ (cd jefferson && sudo python setup.py install)

# Install ubi_reader to extract UBIFS file systems■■■■
$ sudo apt-get install liblzo2-dev python-lzo
$ git clone https://github.com/jrspruitt/ubi_reader
$ (cd ubi_reader && sudo python setup.py install)

# Install yaffshiv to extract YAFFS file systems■■■■
$ git clone https://github.com/devttys0/yaffshiv
$ (cd yaffshiv && sudo python setup.py install)

# Install unstuff (closed source) to extract StuffIt archive files■■■■
```

```
$ wget -O - http://my.smithmicro.com/downloads/files/stuffit520.611linux-i386.tar.gz | tar -zxv
$ sudo cp bin/unstuff /usr/local/bin/
```

qemu安装

```
git clone git://git.qemu.org/qemu.git
cd qemu
git submodule init
git submodule update --recursivesudo
apt install libglib2.0 libglib2.0-devsudo
apt install autoconf automake libtoolcd
■qemu && ./configuremakesudo make install
```

qemu 网络配置

qemu网络配置又有很多坑，google&度娘 各种搜索，终于解决了，解决办法如下。

手动每次配置（启动一次就要配置一次）

```
$ sudo apt-get install uml-utilities
$ sudo tunctl -t tap0 -u sebao
$ sudo ifconfig tap0 172.16.0.1/24

ifconfig tap0
```

进入qemu虚拟机再执行一次命令

```
sudo ifconfig eth0 172.16.0.2/24
```

自动配置

sudo apt-get install uml-utilities

sudo vi /etc/network/interfaces

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
iface br0 inet dhcp
 bridge_ports eth0
 bridge_maxwait 0
```

sebao@ubuntu:~$ sudo cat /etc/default/grub

```
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_HIDDEN_TIMEOUT=0
GRUB_HIDDEN_TIMEOUT_QUIET=true
GRUB_TIMEOUT=10
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash"
GRUB_CMDLINE_LINUX="net.ifnames=0 biosdevname=0"

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
# note that you can use only modes which your graphic card supports via VBE
# you can see them in real GRUB with the command `vbeinfo'
```

```
#GRUB_GFXMODE=640x480

# Uncomment if you don't want GRUB to pass "root=UUID=xxx" parameter to Linux
#GRUB_DISABLE_LINUX_UUID=true

# Uncomment to disable generation of recovery mode menu entries
#GRUB_DISABLE_RECOVERY="true"

# Uncomment to get a beep at grub start
#GRUB_INIT_TUNE="480 440 1"
```

sebao@ubuntu:~$ sudo cat /etc/qemu-ifup

```
#!/bin/sh
echo "Executing /etc/qemu-ifup"
echo "bridge networking"
sudo ifdown eth0
sudo ifup br0
echo "Bringing up $1 for bridge mode"
sudo /sbin/ifconfig $1 0.0.0.0 promisc up
echo "Adding $1 to br0"
sudo /sbin/brctl addif br0 $1
sleep 2
```

配置完一定要重启网卡才能生效

```
sudo /etc/init.d/networking  restart
```

qemu-mips对应包下载

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

我这里下载两个包，这里要对应固件的版本进行下载。这里一定要选择大端和小端。大端和小端是根据固件的架构来选择的。

vmlinux-2.6.32-5-4kc-malta

debian_squeeze_mips_standard.qcow2

启动qemu

qemu-system-mips -M malta -kernel vmlinux-2.6.32-5-4kc-malta -hda debian_squeeze_mips_standard.qcow2 -append "root=/dev/sda1 console=tty0" -net nic,macaddr=52:54:be:36:42:a9 -net tap

D-link dir601 踩坑

解压web目录

```
tar zxvf mnt/www.tgz www/
cp usr/bin/my_cgi.cgi www/
```

直接运行http服务会报各种错误，需要手动创建文件夹，以及文件

创建文件: /var/run/lighttpd.pid

创建文件:/log/lighttpd/error.log

WWW目录下 rt文件夹里面的所有文件，移动到 www目录

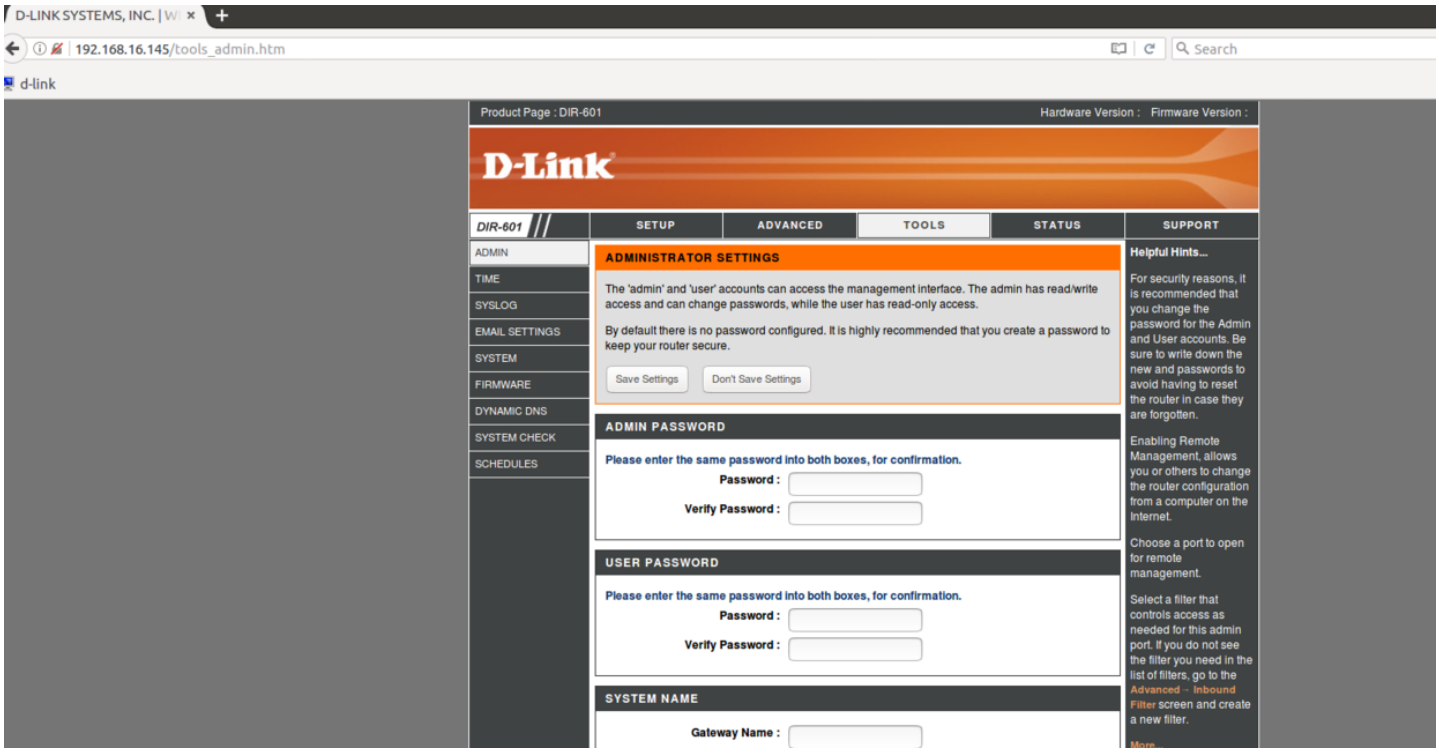
```
chroot . usr/bin/lighttpd -f mnt/lighttpd/lighttpd.conf
57  cd ../
58  ls
59  cd squashfs-root/
60  ls
61  cd www/
62  ls
63  cd ../
64  chroot . usr/bin/lighttpd -f mnt/lighttpd/lighttpd.conf
65  cat mnt/lighttpd/lighttpd.conf | grep "lighttpd.pid"
66  cd var/
67  ls
```

```
68  mkdir run
69  ls
70  cd run
71  vi lighttpd.pid
72  cd ../../
73  chroot . usr/bin/lighttpd -f mnt/lighttpd/lighttpd.conf
77  mkdir log
78  cd log/
79  mkdir lighttpd
80  cd lighttpd/
81  vi error.log
82  cd ../../../
83  chroot . usr/bin/lighttpd -f mnt/lighttpd/lighttpd.conf
84  cd www/
85  ls
86  cd rt/
87  ls
88  cd ../
89  ls
90  ls
91  cd rt/
92  ls
93  ls -ll
94  cd ../
95  mv rt/ .
96  ls
97  mv rt/* .
```

启动固件

```
chroot . usr/bin/lighttpd -f mnt/lighttpd/lighttpd.conf
```

在浏览器输入 qemu虚拟机的ip 就可以进入路由器的界面了。



上一篇：威胁情报真的是网络安全的"少数派报... 下一篇：Tomcat漏洞分析—【CVE-2...

1. 1 条回复

不会c的程序员 2018-11-27 16:05:01

博主您好，我想问一下这个web目录是哪来的啊，我现在有一个dlink的bin文件，已经用binwalk解包了，现在该怎么做啊

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板