

Linux折腾笔记

备忘学到的一点东东，可能同时会方便其他人！

≡ 页 日志 博友 关于我

日志

安装Kali-Linux和Windows构成双系统

cn_windows_8_x64_6in1.iso

Kali-linux安装之后的简单设置

2013-05-24 22:57:54 | 分类：Linux系统 | 标签：kali-linux linux设置

订阅 | 字号



1.更新软件源：

root权限：

leafpad /etc/apt/sources.list

然后添加以下较快的源：

```
deb http://http.kali.org/kali kali main non-free contrib
deb-src http://http.kali.org/kali kali main non-free contrib
deb http://security.kali.org/kali-security kali/updates main contrib non-free
deb http://ftp.sjtu.edu.cn/debian wheezy main non-free contrib
deb-src http://ftp.sjtu.edu.cn/debian wheezy main non-free contrib
deb http://ftp.sjtu.edu.cn/debian wheezy-proposed-updates main non-free contrib
deb-src http://ftp.sjtu.edu.cn/debian wheezy-proposed-updates main non-free contrib
deb http://ftp.sjtu.edu.cn/debian-security wheezy/updates main non-free contrib
deb-src http://ftp.sjtu.edu.cn/debian-security wheezy/updates main non-free contrib
deb http://mirrors.163.com/debian wheezy main non-free contrib
deb-src http://mirrors.163.com/debian wheezy main non-free contrib
deb http://mirrors.163.com/debian wheezy-proposed-updates main non-free contrib
```

```
deb-src http://mirrors.163.com/debian wheezy-proposed-updates main non-free contrib
```

```
deb-src http://mirrors.163.com/debian-security wheezy/updates main non-free contrib
```

```
deb http://mirrors.163.com/debian-security wheezy/updates main non-free contrib
```

保存之后运行：`apt-get update && apt-get dist-upgrade`

2.kali-linux安装中文输入法（以下任意选择一种安装）：

`apt-get install fcitx-table-wbpy ttf-wqy-microhei ttf-wqy-zenhei` #拼音五笔

`apt-get install ibus ibus-pinyin` #经典的ibus

`apt-get install fcitx fcitx-googlepinyin fcitx-pinyin fcitx-module-cloudpinyin` #fcitx拼音

注销，重新登录之后才可以使用。

3.kali-linux安装flash player:

`apt-get install flashplugin-nonfree`

`update-flashplugin-nonfree --install`

4.kali-linux安装qq2012

root权限：

(1) `dpkg --add-architecture i386`

`apt-get update`

`apt-get install ia32-libs libnotify-bin ia32-libs-gtk`

#如果是32位操作系统，这步可以跳过

(2) 下载这个库文件（alsa-lib）：

`http://pan.baidu.com/share/link?shareid=470635&uk=1209563959`

cd到下载目录

`bzip2 -d alsa-lib-1.0.26.tar.bz2 && tar -xvf alsa-lib-1.0.26.tar && cd alsa-lib-1.0.26/ && ./configure && make && make`

`install && make clean`

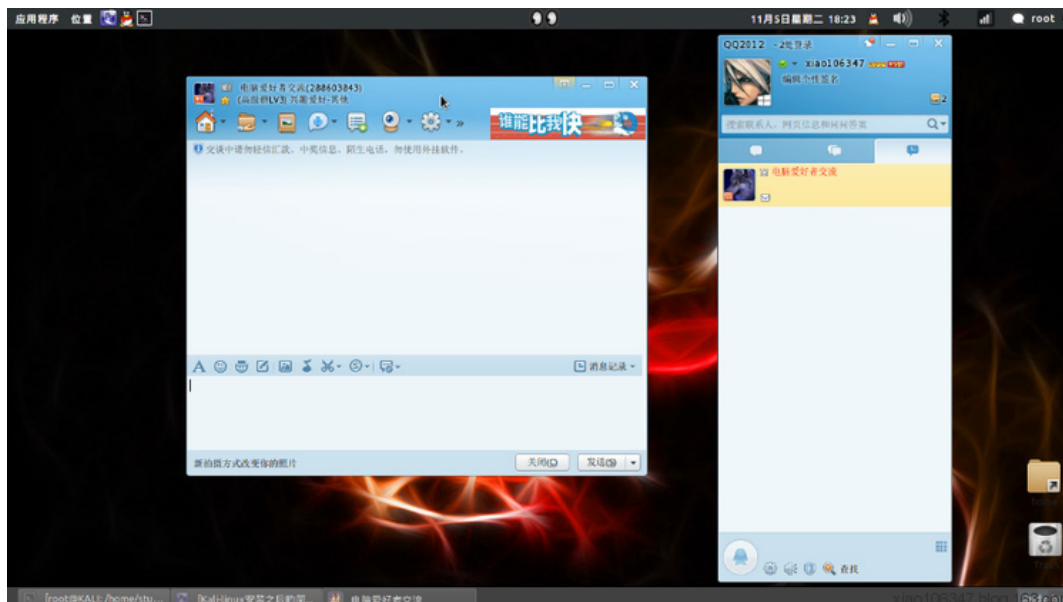
(3) 下载安装wineqq2012:

`wget http://www.longene.org/download/WineQQ2012-20121221-Longene.deb && dpkg -i WineQQ2012-20121221-`

`Longene.deb`

附：**kali-linux安装WineQQ2013:**

<http://xiao106347.blog.163.com/blog/static/215992078201311512333509/>



5.更新并汉化iceweasel

```
deb http://mozilla.debian.net/ wheezy-backports iceweasel-release #添加这个软件源
apt-get install pkg-mozilla-archive-keyring #导入PGP KEY
gpg --check-sigs --fingerprint --keyring /etc/apt/trusted.gpg.d/pkg-mozilla-archive-keyring.gpg --keyring /usr/share/keyrings
/debian-keyring.gpg pkg-mozilla-maintainers #新建钥匙环
apt-get -y update && apt-get install -t wheezy-backports iceweasel && apt-get install iceweasel-l10n-zh-cn
```



5.安装一些工具:

```
apt-get install gnome-tweak-tool #安装gnome管理软件
apt-get install synaptic #安装新立德
apt-get install software-center #安装ubuntu软件中心
apt-get install file-roller #安装解压缩软件
apt-get install audacious #audacious音乐播放器
apt-get install smplayer #安装smplayer视频播放器
apt-get install terminator #安装多窗口终端
```

```
root@KALI: /home/HACKING
-U - do not display unknown signatures
-K - do not display known signatures (for tests)
-S - report signatures even for known systems
-A - go into SYN+ACK mode (semi-supported)
-R - go into RST/RST+ACK mode (semi-supported)
-O - go into stray ACK mode (barely supported)
-r - resolve host names (not recommended)
-q - be quiet - no banner
-v - enable support for 802.1Q VLAN frames
-p - switch card to promiscuous mode
-d - daemon mode (fork into background)
-l - use single-line output (easier to grep)
-x - include full packet dump (for debugging)
-X - display payload string (useful in RST mode)
-C - run signature collision check
-t - add timestamps to every entry

'Filter rule' is an optional pcap-style BPF expression (man tcpdump).
root@KALI: /home/study# p0f
p0f - passive os fingerprinting utility, version 2.0.8
(C) M. Zalewski <lcantuf@diene.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN) on 'eth0'. 262 sigs (14 generic, cksum 0F1F5CA2), rule: 'all'.

-udev- 2*[udev]
-udisks-daemon- 2*[udisks-daemon]
-upower- 2*[upower]
-vmactool- 2*[vmactool]
-vmnet-bridge- 2*[vmnet-bridge]
-vmnet-dhcpd- 2*[vmnet-dhcpd]
-vmnet-natd- 2*[vmnet-natd]

tion Service Pack 5" (Guess probability: 83%)
[+] Host 115.239.210.27 Running OS: "Apple Mac OS X 10.4.0" (Guess probability: 83%)
[+] Host 115.239.210.27 Running OS: "Cisco IOS 11.1" (Guess probability: 83%)
[+] Host 115.239.210.27 Running OS: "Cisco IOS 12.3" (Guess probability: 83%)
[+] Host 115.239.210.27 Running OS: "Cisco IOS 11.3" (Guess probability: 83%)
[+] Host 115.239.210.27 Running OS: "Cisco IOS 12.0" (Guess probability: 83%)
[+] Host 115.239.210.27 Running OS: "Cisco IOS 12.2" (Guess probability: 83%)
[+] Host 115.239.210.27 Running OS: "Cisco IOS 11.2" (Guess probability: 83%)
[+] Host 115.239.210.27 Running OS: "Apple Mac OS X 10.4.1" (Guess probability: 83%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
root@KALI: /home#

软件包未被升级。
解压缩后将会空出 158 kB 的空间。
您希望继续执行吗？[Y/n]y
正在读取数据库... 系统当前共安装有 307961 个文件和目录。
正在卸载 mtr...
正在处理用于 man-db 的触发器...
正在处理用于 menu 的触发器...
root@KALI: /usr/bin# apt-get autoremove
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
升级了 0 个软件包，新安装了 0 个软件包，要卸载 0 个软件包，有 0 个软件包未被升级。
root@KALI: /usr/bin#
```

6.开启gnome 3的标准模式：

`gsettings set org.gnome.desktop.session session-name gnome`

#这个模式比较流畅

`gsettings set org.gnome.desktop.session session-name gnome-fallback`

#还原默认模式

`gnome-shell -replace`

#在默认模式临时开启

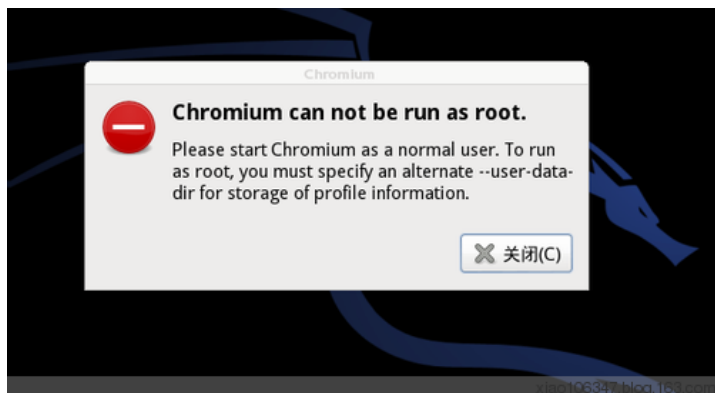
经典模式：



7.kali安装chromium浏览器：

`apt-get install chromium-browser`

此时可以在应用程序-互联网下面找到chromium，如果是普通用户，可以立即使用，如果当前是root账户登录的系统，打开chromium提示Chromium can not be run as root：



解决linux下root账户无法打开chromium的方法：右键桌面chromium图标，选属性;或打开主菜单，找到chromium，点属性：



往命令框之后添加一个空格，然后再添加`--user-data-dir $HOME, close`

这是完整命令：`/usr/bin/chromium %U --user-data-dir $HOME, close`

也可以把`--user-data-dir $HOME`写入`/usr/bin/chromium`文件的尾部，这样彻底些

同样，安装`google-chrome`也是一样的（`/usr/bin/google-chrome`）

关闭之后就可以打开了！



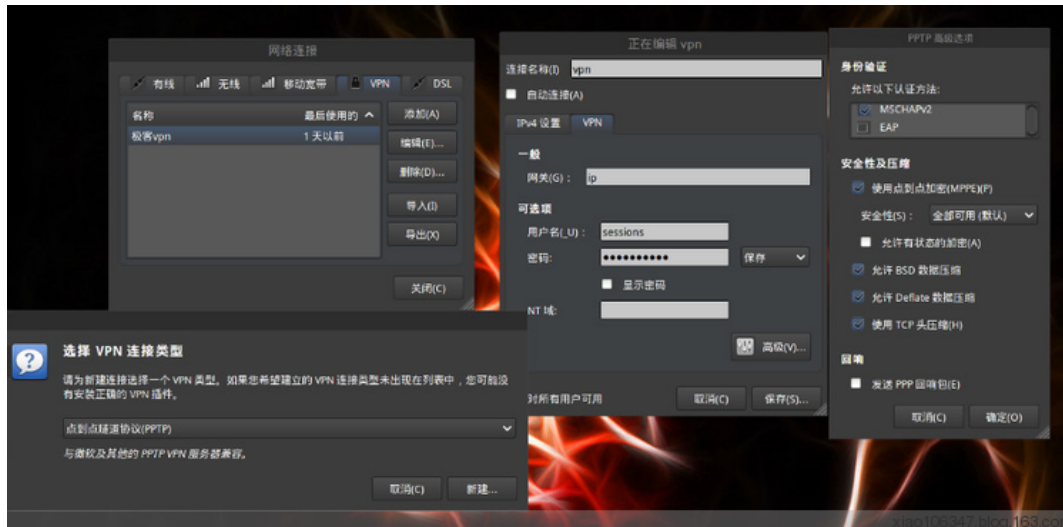
8.Kali-linux设置vpn代理：

依次执行以下命令之后就可以陪置vpn了：

```
apt-get install network-manager-openvpn-gnome
```

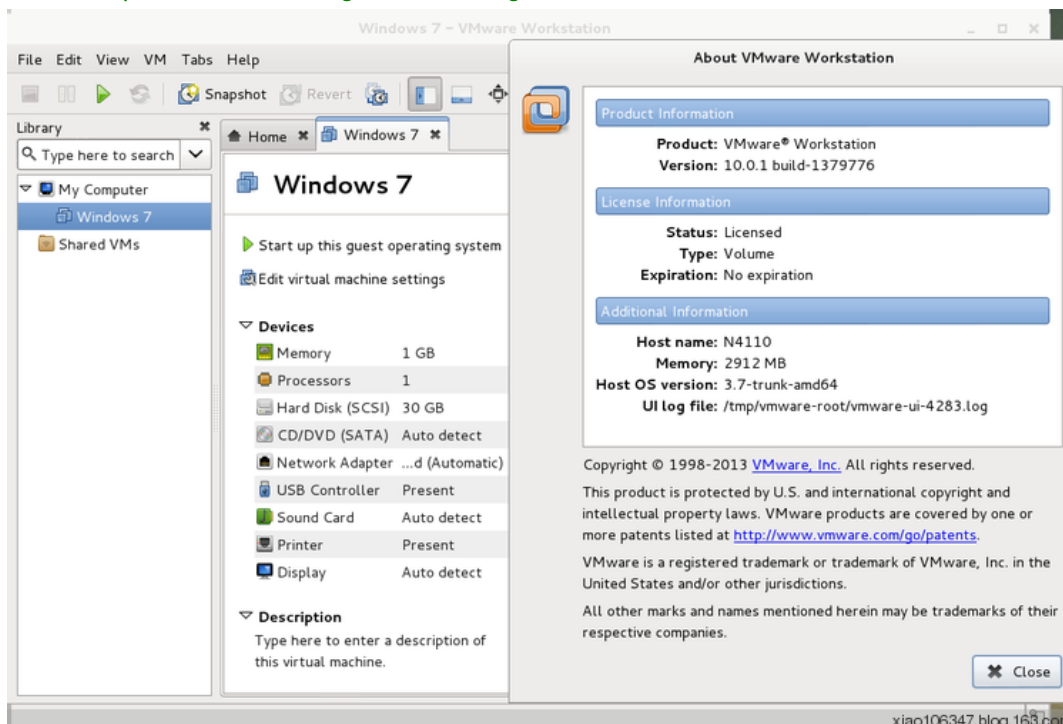
```
apt-get install network-manager-pptp
```

```
apt-get install network-manager-pptp-gnome
apt-get install network-manager-strongswan
apt-get install network-manager-vpnc
apt-get install network-manager-vpnc-gnome
/etc/init.d/network-manager restart
```



9. 安装VMware和VirtualBox

链接: <http://xiao106347.blog.163.com/blog/static/2159920782013928288628/>



10.运行 Metasploit Framework(转, 原文地址: <http://www.backtrack.org.cn/thread-12664-1-1.html>)

依照kali linux网络服务策略,Kali没有自动启动的网络服务,包括数据库服务在内。所以为了让metasploit以支持数据库的方式运行有些必要的步骤。

启动Kali的PostgreSQL服务: Metasploit 使用PostgreSQL作为数据库,所以必须先运行它。

```
service postgresql start
```

可以用ss -ant的输出来检验PostgreSQL是否在运行,然后确认5432端口处于listening状态。

State Recv-Q Send-Q Local Address:Port Peer Address:Port

LISTEN 0 128 :::22 :::*8

LISTEN 0 128 *:22 *:3

LISTEN 0 128 127.0.0.1:5432 *:4

LISTEN 0 128 ::1:5432 :::*

启动Kali的Metasploit服务：随着PostgreSQL的启动和运行，接着我们要运行Metasploit服务。第一次运行服务会创建一个msf3数据库用户和一个叫msf3的数据库。还会运行Metasploit RPC和它需要的WEB 服务端。

service metasploit start

在Kali运行msfconsole：现在PostgreSQL 和 Metasploit服务都运行了，可以运行 msfconsole，然后用 db_status 命令检验数据库的连通性。

msf > db_status

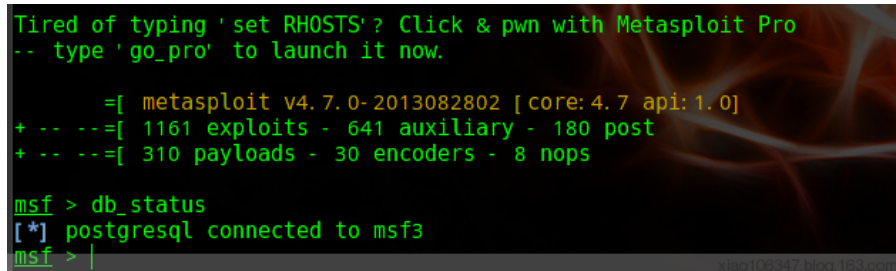
[*] postgresql connected to msf3

msf >

配置Metasploit随系统启动运行：如果你想PostgreSQL和Metasploit在开机时运行，你可以使用update-rc.d启用服务。

update-rc.d postgresql enable

update-rc.d metasploit enable



附：[metasploit连接数据库](http://xiao106347.blog.163.com/blog/static/2159920782013101224632205/)：http://xiao106347.blog.163.com/blog/static/2159920782013101224632205/

xiao106347推荐阅读：



推荐 3人 | 分享到：

阅读(6703) | 评论(5) | 转载 (0) | 举报

安装Kali-Linux和Windows构成双系统

cn_windows_8_x64_6in1.iso

最近读者



评论

点击登录 | 昵称:



ghos

11-21 16:33

十分感谢！很有用，学到了很多！

回复



东吃

11-19 18:15

xiexie

回复



乖乖天才

10-19 20:16

写得不错，学习了！谢谢楼主！

回复



6522宿舍

09-21 09:45

很不错

回复



xiao106347 回复 6522宿舍

09-21 21:46

谢谢支持🙏

回复

[公司简介](#) - [联系方法](#) - [招聘信息](#) - [客户服务](#) - [隐私政策](#) - [博客风格](#) - [手机博客](#) - [VIP博客](#) - [订阅此博客](#)

网易公司版权所有 ©1997-2013