Kali 2.0 安装与使用指南

Kali 如今都已经 2.0 版本了，不，准备说是 kali 滚动更新版了，因此我总结了我自己在搭建 kali（硬盘安装）的最新方法，以及可能出现的问题的解决方案，力求给大家一个最新的，最接近正确配置的 kali 过程，如有不妥或者其他想法欢迎指出。

1、 系统更新

安装好 kali 之后更新源是第一大问题，官方的源速度又很慢，刚装好的 kali 又不能科学上网，因此补充源很重要，我总结了国内外很多源。如下：（个人测试过 kali 最新滚动版的源，如果你提前配置好科学上网更新还好，如果没有提前配置的话他的官网源有很多会丢包，如果你真是想用最新版的话，具体更新源的方法官网有。）

首先：root@kali:~# leafpad /etc/apt/sources.list，然后将以下源复制进去保存。

#kali 官方源

deb cdrom:[Debian GNU/Linux 2.0 _Sana_ - Official Snapshot i386 LIVE/INSTALL Binary 20150811-09:06]/ sana contrib main non-free

deb cdrom:[Debian GNU/Linux 2.0 _Sana_ - Official Snapshot i386 LIVE/INSTALL Binary 20150811-09:06]/ sana contrib main non-free

deb http://http.kali.org/kali sana main non-free contrib

deb-src http://http.kali.org/kali sana main non-free contrib

deb http://security.kali.org/kali-security/ sana/updates main contrib non-free

deb-src http://security.kali.org/kali-security/ sana/updates main contrib non-free

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

#阿里云 Kali 源

deb http://mirrors.aliyun.com/kali kali main non-free contrib

deb-src http://mirrors.aliyun.com/kali kali main non-free contrib

deb http://mirrors.aliyun.com/kali-security kali/updates main contrib non-free

#kali 新加坡源的地址

deb http://mirror.nus.edu.sg/kali/kali/ kali main non-free contrib

deb-src http://mirror.nus.edu.sg/kali/kali/ kali main non-free contrib

deb http://security.kali.org/kali-security kali/updates main contrib non-free

deb http://mirror.nus.edu.sg/kali/kali-security kali/updates main contrib non-free

deb-src http://mirror.nus.edu.sg/kali/kali-security kali/updates main contrib non-free

#debian_wheezy 国内源的地址

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

#中科大 kali 源

deb http://mirrors.ustc.edu.cn/kali kali main non-free contrib

deb-src http://mirrors.ustc.edu.cn/kali kali main non-free contrib

deb http://mirrors.ustc.edu.cn/kali-security kali/updates main contrib non-free

然后更新并安装

root@kali:~# apt-get update && apt-get dist-upgrade

2、安装内核头（作用装显卡驱动或者虚拟机增强工具会用到。）

root@kali:apt-get install linux-headers-$(uname -r)

注：如果报错了的话可以输入这个试试

aptitude -r install linux-headers-$(uname -r

如果是报未找到的错误你就要看看源是否有问题，复制我的源就可以了。

3、 安装浏览器

我建议安装谷歌浏览器是因为系统自带的是 iceweasel（就相当于火狐），这样的话你渗透测试浏览器的插件你就可以都能安装起来，并且如果科学上网使用 lantern 的话兼容性好点，关于浏览器这面很容易出现几个问题，我分别介绍下：

（1）如果坚持用系统自带浏览器，其汉化方法：

答：root@kali:apt-get install iceweasel-l10n-zh-cn

（2）如果有强迫症删了系统自带浏览器，然后重新安装了一个新的火狐可能遇到的问题：

答：可能会出现 gnome 桌面被误删，从而导致系统进不去，并且即使你安装了一个新的火狐然后你就卸载不了了，会一直提示报错，并且此时如果你还想安装其他浏览器的话也会报错，如果真遇到的话你又不想重装系统有个治标不治本的方法（root@kali:sudo apt-get install –reinstall firefox-mozilla-build），还有说道如果桌面崩溃处理方法就是 ctrl+alt+Fn(数字)进入非图形化界面然后重新安装下桌面环境。

（3）如果你有火狐账号，你登陆了发现书签和插件没有同步？

答：可能是你原先用的是火狐国内版，而 kali 里面的是国际版的，因此不能同步，网上搜索过有人说同步插件让书签同步，但是我测试多次没成功过。

（4）安装谷歌浏览器

答：官网上下载谷歌浏览器（可能你访问不了，有时候等等还是可以出现下载链接的，如果访问不了去百度上搜索下然后下载个 deb 包），然后到下载目录安装下：root@kali:dpkg -i google-chrome-stable（具体以实际包的名称为准）。安装完之后，如果你是 root 运行，会提示你不给 root 执行的。解决方法：root@kali:gedit /usr/bin/google-chrome，然后在最后一行尾加入–user-data-dir（注意空格喔）。

（5）安装 flash

答：首先 root@kali:apt-get install flashplugin-nonfree

其次 root@kali:update-flashplugin-nonfree –install

(6)安装 tor（看个人喜好）

答：

root@kali:apt-get install tor

root@kali:service tor start

root@kali:proxychains iceweasel

4、 安装中文输入法

Kali 自带是不能输入中文的，因此我安装了搜狗输入法和谷歌输入法（我做备份的），安装其一便可以。建议安装前 apt-get update 下，刷新下。其次安装好任意输入法需要重启下才能正常打字（ctrl+空格）

apt-get install fcitx

apt-get install fcitx-googlepinyin //安装谷歌拼音

搜狗打字去官网下载 deb，然后 dpkg -i 安装对应搜狗包 //安装搜狗拼音

5、安装百度云

（以最常用云盘为例，其他云盘有的也有 linux 版本）

首先先 git 一下：https://github.com/LiuLang/bcloud-packages

然后安装自己对应版本（32bit or 64bit）

dpkg -i bcloud-x.x.x.debapt-get -f install

6、安装 WPS

首选官网下载 deb 包：http://community.wps.cn/download/

其次对应下载位置 dpkg -i 安装下即可。

7、安装 dota2 和 steam 平台

（64 位适合）【广告下:dota1 选手，欢迎球带..】

首选官网下载 steam 并且 dpkg 安装下 然后如果你是 root 运行会有提示。解决方法终端执行：

/usr/bin

gedit steam

Don’ t allow running as rootif ["$(id -u)" == "0"];

thenshow_message –error $”Cannot run as root user”exit 1

Fi

然后找到如上位置，并且把双引号中的 0 改成 1 即可

然后登陆账号，下载 dota2，然后就没有然后啦。。。

8、安装网易云音乐

首先 git 下 https://github.com/cosven/FeelUOwn

然后下载后依次输入

root@kali:git clone https://github.com/cosven/FeelUOwn.git

root@kali:cd FeelUOwn

root@kali:./install.sh

注：遇到有什么依赖没有安装，根据提示缺少什么依赖安装什么依赖即可。

9、安装代码编辑器

（个人喜好）首先安装比较容易，官网下载然后 dpkg 下就 ok 了，安装好之后 submit text 下面不能输入中文需要解决，其次如果要汉化界面那汉化包要找一会。。）

解决不能输入中文方法：

（1）新建并保存下面的代码为 sublime_imfix.c

/*

sublime-imfix.c

Use LD_PRELOAD to interpose some function to fix sublime input method support for linux.

By Cjacker Huang

gcc -shared -o libsublime-imfix.so sublime_imfix.c `pkg-config --libs --cflags gtk+-2.0` -fPIC

LD_PRELOAD=./libsublime-imfix.so sublime_text

*/#include #include typedef GdkSegment GdkRegionBox;

struct _GdkRegion

{

long size;

long numRects;

GdkRegionBox *rects;

GdkRegionBox extents;

};

GtkIMContext *local_context;

voidgdk_region_get_clipbox (const GdkRegion *region,

GdkRectangle *rectangle){

```
        g_return_if_fail (region != NULL);
        g_return_if_fail (rectangle != NULL);

        rectangle->x = region->extents.x1;
        rectangle->y = region->extents.y1;
        rectangle->width = region->extents.x2 - region->extents.x1;
        rectangle->height = region->extents.y2 - region->extents.y1;
        GdkRectangle rect;
        rect.x = rectangle->x;
        rect.y = rectangle->y;
        rect.width = 0;
        rect.height = rectangle->height;
        //The caret width is 2;    //Maybe sometimes we will make a mistake,
but for most of the time, it should be the caret.   if(rectangle->width ==
2 && GTK_IS_IM_CONTEXT(local_context)) {
                gtk_im_context_set_cursor_location(local_context, rectangle);
        }
    }
     //this is needed, for example, if you input something in file dialog
and return back the edit area//context will lost, so here we set it
```

again. static GdkFilterReturn event_filter (GdkXEvent *xevent, GdkEvent *event, gpointer im_context){

```
        XEvent *xev = (XEvent *)xevent;
        if(xev->type == KeyRelease &&
GTK_IS_IM_CONTEXT(im_context)) {
            GdkWindow * win =
g_object_get_data(G_OBJECT(im_context),"window");
            if(GDK_IS_WINDOW(win))
              gtk_im_context_set_client_window(im_context, win);
        }
        return GDK_FILTER_CONTINUE;
    }
     void gtk_im_context_set_client_window (GtkIMContext *context,
                GdkWindow     *window){
       GtkIMContextClass *klass;
       g_return_if_fail (GTK_IS_IM_CONTEXT (context));
       klass = GTK_IM_CONTEXT_GET_CLASS (context);
       if (klass->set_client_window)
         klass->set_client_window (context, window);
```

```
    if(!GDK_IS_WINDOW (window))
      return;
    g_object_set_data(G_OBJECT(context),"window",window);
    int width = gdk_window_get_width(window);
    int height = gdk_window_get_height(window);
    if(width != 0 && height !=0) {
      gtk_im_context_focus_in(context);
      local_context = context;
    }
    gdk_window_add_filter (window, event_filter, context);
  }
```

2. 编译动态库

gcc -shared -o libsublime-imfix.so sublime_imfix.c `pkg-config --libs --cflags gtk+-2.0` -fPIC

3.设置 LD_PRELOAD 并启动 Sublime Text：

LD_PRELOAD=./libsublime-imfix.so sublime_text

解决界面汉化：网上搜索下载 Sublime_Text_CN_3059.zip，解压之后得到 Default.sublime-package 文件，其实就是个 package，在菜单中选择 preferences——Browse packages 进入到 /home/siat/.config/sublime-text-3/Packages 然后向上一级进入到 /home/siat/.config/sublime-text-3/Installed Packages，把

Default.sublime-package 包复制到 Installed Packages 文件夹下，这时 sublime text3 立刻变成中文了。

其他编辑器安装（由于我没有测试过，仅复制链接为各位省去搜索时间）

安装 eclipe 及 pydev,django

可参考 http://blog.csdn.net/allen_zhao_2012/article/details/7988389

首先

apt-get install -y eclipse

默认安装的 eclipse plugins 路径为: /usr/lib/eclipse/

其次下载 pydev

wget http://downloads.sourceforge.net/project/pydev/pydev/PyDev%203.2.0/PyDev%203.2.0.zip?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fpydev%2Ffiles%2Fpydev%2FPyDev%25203.2.0%2F&ts=1407645058&use_mirror=cznic

最后

unzip PyDev\ 3.2.0.zip

cp -r features /usr/lib/eclipse/cp -r plugins /usr/lib/eclipse/

最最后

打开 eclipse

Windows → Preferences → PyDev → Python Interpreters →

(可以 Auto config 也可手动)

Interpreter name: Python 2.73 Interpreter Executable: /usr/bin/python2.7/usr/bin/python2.7

安装 django:

curl https://bootstrap.pypa.io/ez_setup.py -o - | python

apt-get install -y apache2 libapache2-mod-wsgi mysql-server python-mysqldb

下载 django: #下载页面 https://www.djangoproject.com/download/

wget https://www.djangoproject.com/download/1.6.5/tarball/

tar -zxvf Django-1.6.5.tar.gzcd Django-1.6.5python setup.py install

10、安装 add-apt-repository 和 pip

add-apt-repository

apt-get install python-software-properties

nano app-apt-repository.sh

#!/bin/bash // 添加如下代码 if [$# -eq 1]

NM=`uname -a && date`

NAME=`echo $NM | md5sum | cut -f1 -d" "`

或者其他方法：

http://www.blackmoreops.com/2014/02/21/kali-linux-add-ppa-repository-add-apt-repository/ Pip

apt-get python-setuptools

easy_install pip

pip gevent --upgrade

注：如果最后一步出错，执行 root@kali:pip install setuptools --no-use-wheel --upgrade

11、科学上网

（1）默认安装，是没有激活 VPN 的，能看到 VPN 选项，但是不能点击 VPN 连接

apt-get install -y pptpd network-manager-openvpn network-manager-openvpn-gnome network-manager-pptp network-manager-pptp-gnome network-manager-strongswan network-manager-vpnc network-manager-vpnc-gnome

（1）lantern https://github.com/getlantern/lantern-binaries

方法就是下载对应的版本，然后 dpkg 安装下，然后打开 lantern 自动跳转到浏览器，然后就没有然后了。。。

（2）其次还有就是 ss

首先搭建 shadowsocks 客户端

git 下 https://github.com/shadowsocks/shadowsocks-qt5 以及其安装指南

https://github.com/shadowsocks/shadowsocks-qt5/wiki/%E5%AE%89%E8%A3%85%E6%8C%87%E5%8D%97

或者直接用 pip 安装

pip install shadowsocks

/usr/local/python/bin/sslocal //ss 位置

建立一个为 ss.conf 的配置文件

{

"server" : "100.100.100.100",

"server_port" : 8888,

"local_port" : 1080,

"password" : "123456",

"timeout" : 600,

"method" : "aes-256-cfb"}

然后运行

sslocal -c /filepath/ss.conf

其次安装 privoxy 实现 socks5 转换成 http

privoxy-3.0.23-stable-src.tar.gz //http://www.privoxy.org/官网下载源码

tar xf privoxy-3.0.23-stable-src.tar.gz　//解压缩 cd privoxy-3.0.23-stable

useradd privoxy　//进入目录后创建 privoxy 用户 ,然后安装 autoheader && autoconf

./configure

make && make install

Vim /usr/local/etc/privoxy/config　修改配置文件

listen-address 127.0.0.1:8118　//找到 783 行，去掉注释即可

forward-socks5t / 127.0.0.1:1080.　//找到 1336 行，去掉注释即可，保证 1080 端口和 ss 配置中一致，注意 1080 后面与个小数点。

最后让终端走代理

vim /ect/profile

添加一下两行

export http_proxy=http://127.0.0.1:8118export ftp_proxy=http://127.0.0.1:8118

然后打开 shadowsocks privoxy

sslocal -c /filepath/ss.conf

service privoxy start

测试 curl www.google.com

访问谷歌即可，如果不行查看配置或者重启下。

12、安装 wine 以及 qq

(我是 32 位，如果是 64 位要配置下 32 位架构，还有 wine 感觉靠 rp)

sudo add-apt-repository ppa:ubuntu-wine/ppa

sudo apt-get updatesudo apt-get install wine

Wine 安装好了之后，qq 只要下载我共享目录中的 qq 三个文件即可。（注：qq 安装后有的会提示版本过久，或者安装后不能用。我自己用的 7.8 版本，由于上传太慢就不 gx 了，网上搜搜也能搜到的)

13、Kali 下安装虚拟机

首先先下载

https://download3.vmware.com/software/wkst/file/VMware-Workstation-Full-10.0.2-1744117.i386.bundle

然后给修改权限

chmod u+x VMware-Workstation-Full-10.0.2-1744117.i386.bundle

./Mware-Workstation-Full-10.0.2-1744117.i386.bundle

注意: ./vmware 提示 before run vmware xxxxxxxxxxxxx

出现这样的问题，就是没有安装对应内核的开发包

apt-get install linux-headers-xxxxxxxxxxxxxxxxxxx tab huigei tips

debian 的话安装 linux-headers 就行了，确实没有“kernel-devel”

stable 的话

apt-get install linux-headers-xxxxxxxxxxxxxxxx

其他的比如 vbox，或者是 docker 等均官网有方法。

14.系统优化、美化

（1）Kali2.0 自带了 gnome-tweak-tool，然后网上下载对应的美化内容即可打造自己喜欢的环境（对于强迫症的我来说不美化到我习惯操作真不舒服的）

https://wiki.archlinux.org/index.php/GNOME_%28%E7%AE%80%E4%BD%93%E4%B8%AD%E6%96%87%29

（2）以及桌面环境如果不喜欢 gnome 即可换其他的，个人比较推荐 xfce 吧，轻捷- -

http://cn.docs.kali.org/live-build-cn/%E5%AE%9A%E5%88%B6kali%E7%9A%84%E6%A1%8C%E9%9D%A2%E7%B3%BB%E7%BB%9F

（3）安装新立得软件管理器（个人喜好）

apt-get install synaptic //一款图形化管理软件的管理器

（4）添加用户和设置快捷键（个人喜好）

添加个普通用户方便系统稳定性，设置快捷键方便自己习惯，我快捷键主要修改两个输入法和 shell 窗口，比如：shell 窗口启动终端快捷键

系统》设置》快捷键

添加如下命令：

gnome-terminal

然后输入自己喜好的，我输入的是 CTRL+R。

15 、系统备份

或者使用 dd 之类命令

tar cvpzf backup.tgz --exclude=/proc --exclude=/lost+found --exclude=/backup.tgz --exclude=/mnt --exclude=/sys --exclude=/media /

注意：如果在安装的时候你把没有分磁盘，dd 命令备份你没有地方保存（大移动硬盘者当我没说。。。）