windows密码绕过工具

2020-05-15 翱翔的真爱 来源 审核中 修改

一. 介绍

Kon-Boot是一款专业的多平台密码绕过工具，支持Windows和macOS的多个版本，其中包括Windows XP到Windows 10的所有版本。

目前有很多类似密码绕过工具，这些是通过移除windows账户，修改并可能不安全地覆盖windows密码存储文件等方式来实现的。(如WinPassKey, PassMoz LabWin, iSeePassword, PCUnlocker等)

而Kon-Boot的特点就在于它不会去擦除windows密码，不会修改windows文件，这使得Kon-Boot的使用更加安全。此外，Kon-Boot的最新版是目前世界上唯一的一个能够绕过Windows 10在线密码的方案。

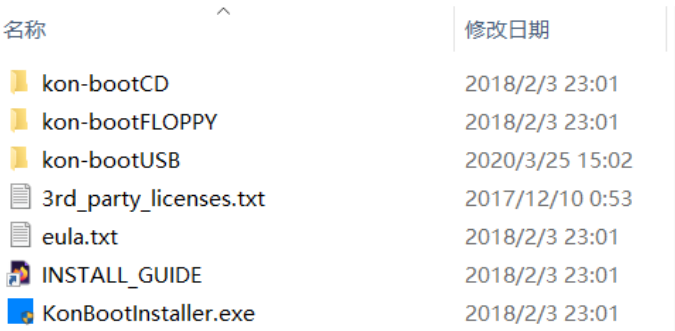
Kon-Boot的原理是在启动时暂时改变系统内核的引导处理，跳过SAM检查，让你在登录界面输入任何字符即可登录，在下一次不用Kon-Boot启动电脑时，原来的密码还是会生效，因为之前暂时的改变会被系统丢弃。

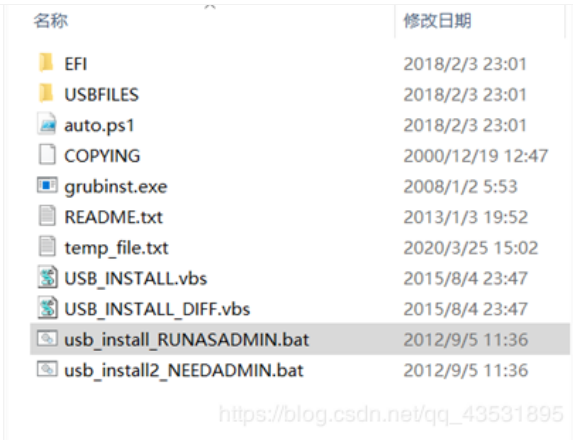
二. 安装

Kon-Boot 2.7 :

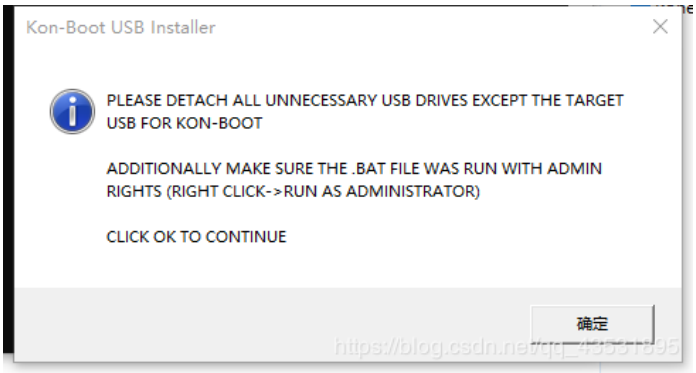
先插上U盘，因为可能会覆盖U盘内容，所以应该预先做一个备份。

下载解压后，Kon-Boot的目录结构是这样的



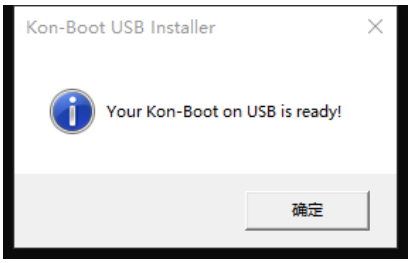


接下来应该会出现下图，让你确认只有这一个USB存储设备。



确定后如下，

再次确认后，过几秒钟Kon-Boot就安装成功了，如下图。（注意这里可能因为个别电脑的问题会不成功，我就是grldr文件复制不了，后来换了一台电脑就成功了）

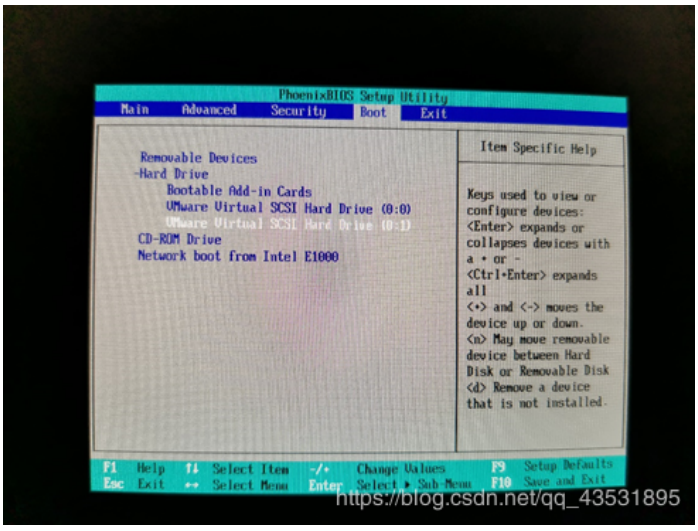


三. Windows平台使用方法

这里测试了win 7和win 10两个版本

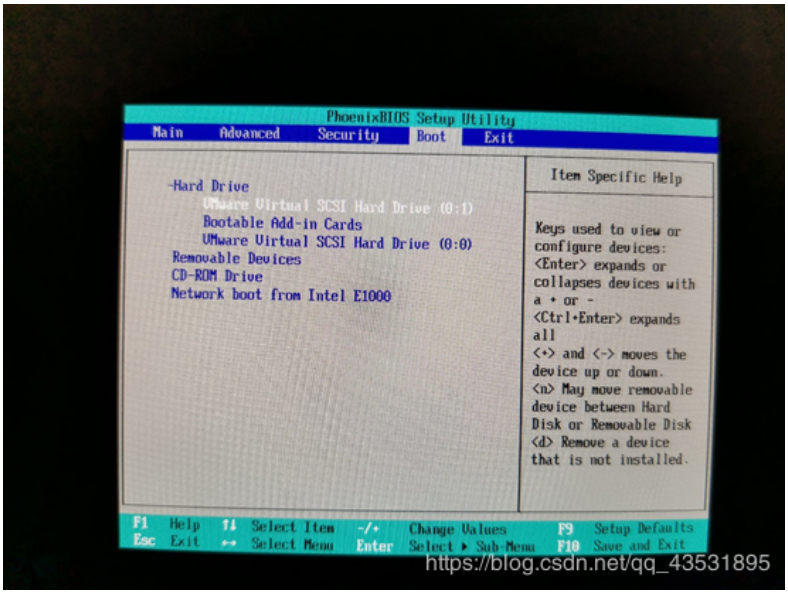
1. Win 7

然后在Boot下将启动首选项设置为U盘启动，Boot菜单如图



这里最下面的VMware Virtual SCSI Hard Drive就是新加的U盘。（正常的物理机这里应该是USB设备，由于我使用的是VMware虚拟机进行实验，U盘是作为新加硬盘配置的，所以这里是Hard Drive，具体配置方法后面会详细介绍）

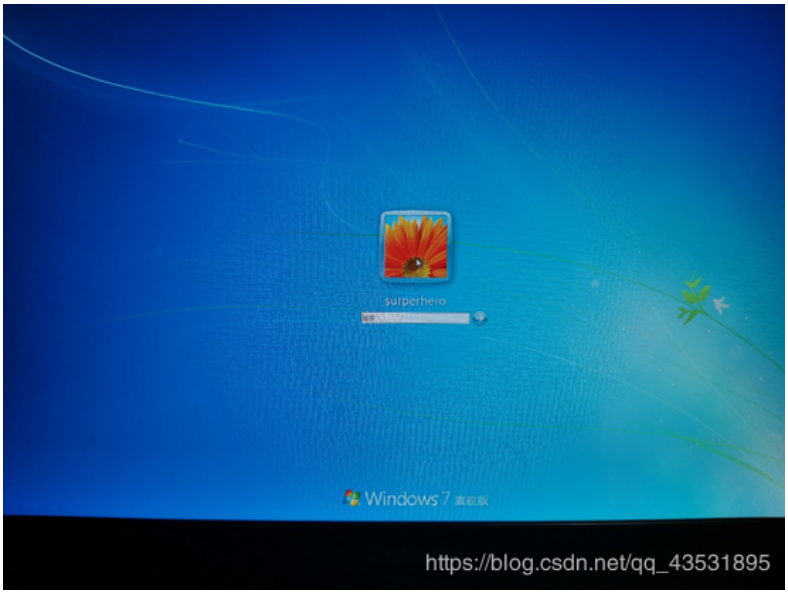
设置方法为，按住shift后再按+号，就会使目标上移，将目标移到最顶部即可，如图。



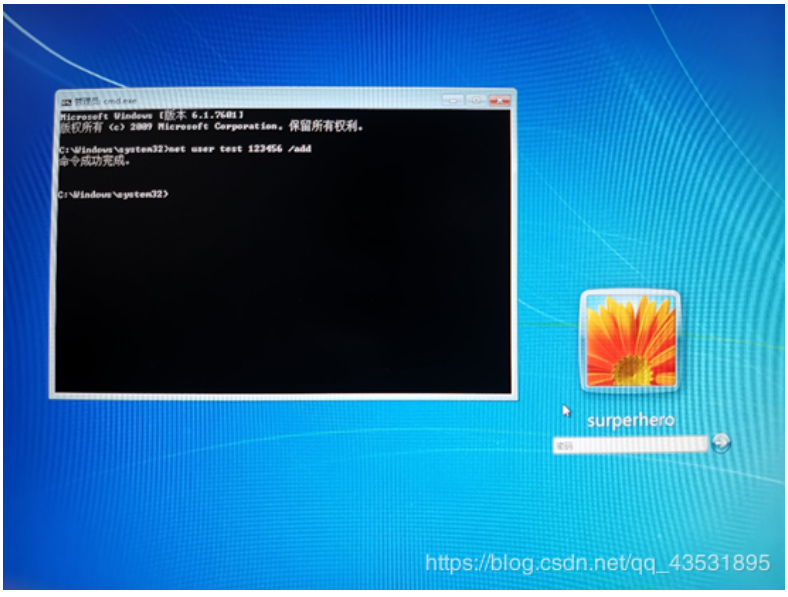
然后按F10保存退出，就进入kon-boot界面

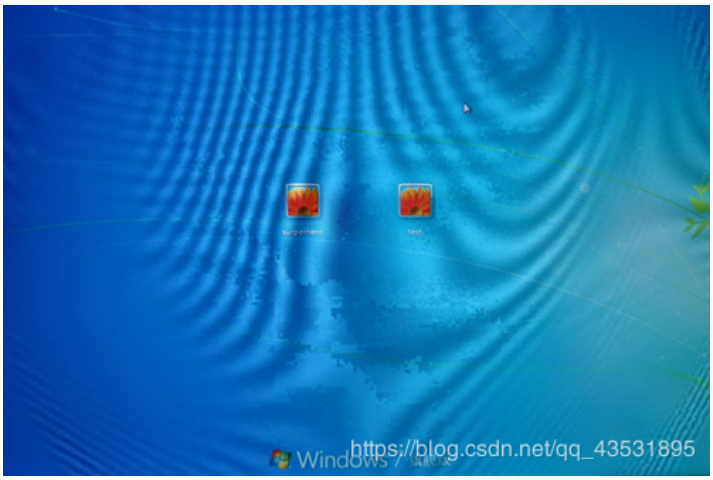
选择第一个，回车就会开始打印kon-boot的logo

打印完成后就会进入windows登陆页面，不用输入密码，直接回车就可以进去。



或者这里可以连按5次shift，可以出现具有管理员权限的cmd窗口，使用
Net user <用户名> <密码> /add 命令，
可以创建windows访客账号。





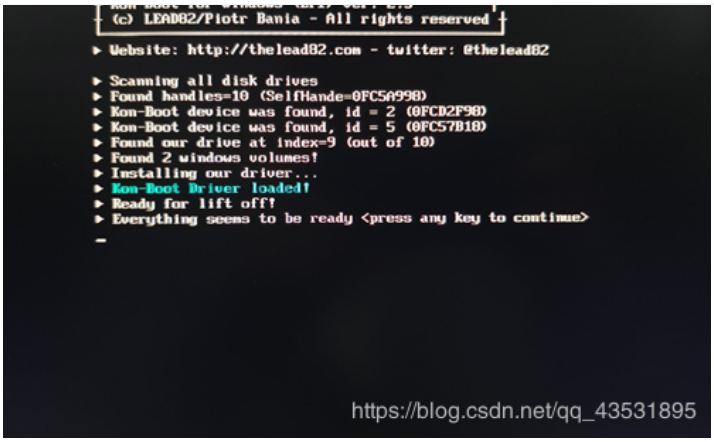
2. Win 10

同样在开机前插上u盘，开机时连续按F2进入BIOS（不同主板方法可能不同）

在Boot manager中选择启动项，如图

图中的最下面的EFI VMware Virtual SCSI Hard Drive即为新加U盘（正常物理机应该是USB设备，我这里同样使用VMware虚拟机进行实验）

用上下键选中目标后回车即可进入kon-boot界面

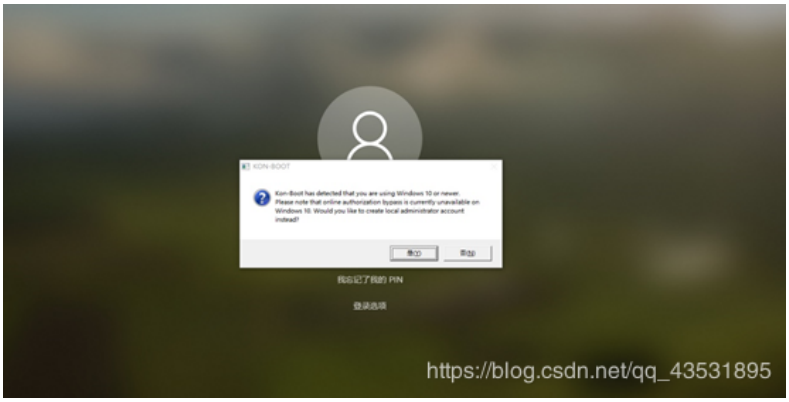


任意按一个键后进入如下界面，这里输入y即可，即是选择第一个

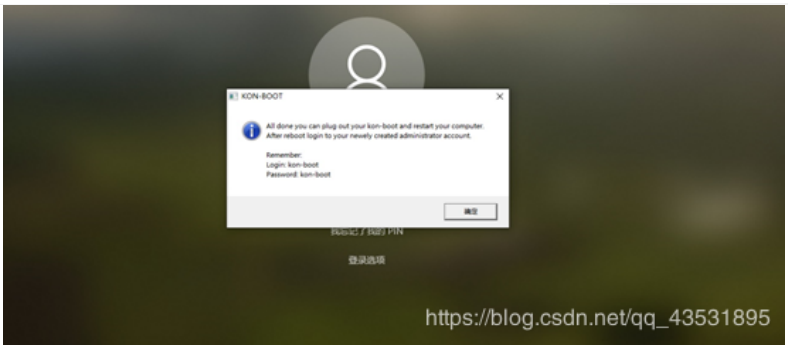
然后应该会直接进入windows登陆界面，不过我在实验时候总是会出现“press any key to boot from CD or DVD”，然后出现Boot manager，我明明选择的是硬盘启动，怎么会出现CD or DVD的提示……

不过经过多次测试后，发现这里再选择Boot normally即可正常启动kon-boot，进入windows登陆页面。

在登陆页面，kon-boot会弹出弹窗，检测到你的系统是win 10，由于我这个版本的还不支持win 10的在线密码绕过，不过它会帮你创建一个新的本地管理员账号。



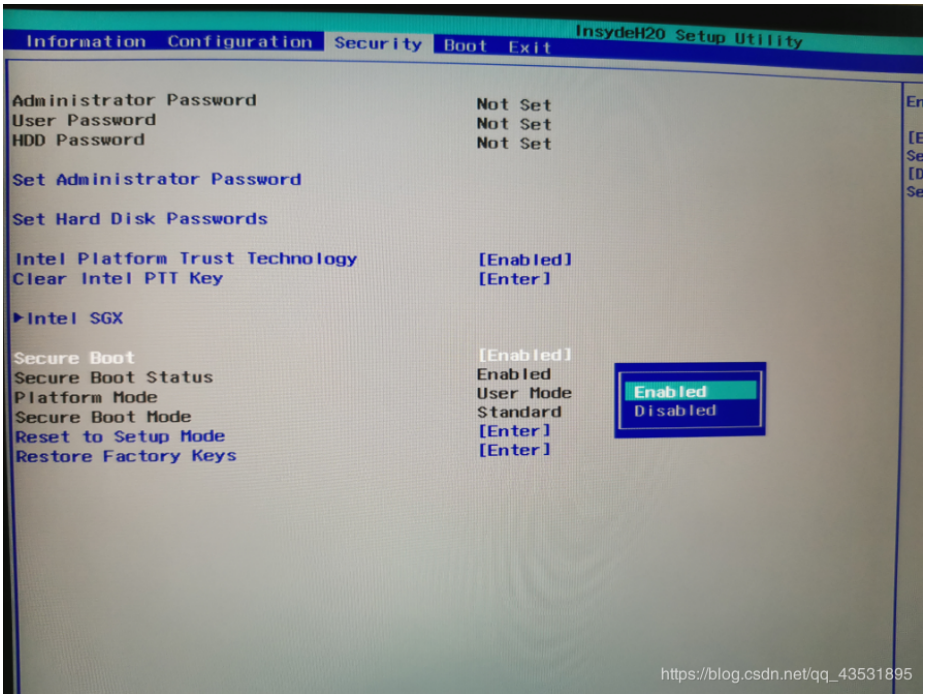
确认后，如图，新的本地管理员账号密码都是kon-boot



然后重启电脑就可以使用kon-boot账号登陆windows。

3.注意

使用kon-boot时，关键是要进入BIOS关掉Secure Boot（如图），并且设置以U盘启动。



在实验中本来想测试一个华硕主板的物理机，但是华硕主板在关掉Secure Boot后会出现安全登录警报，无法继续进行，在打开Secure Boot后又会提示没有开启UEFI模式，也无法继续进行，不知道华硕主板该怎么设置。

四. 提权

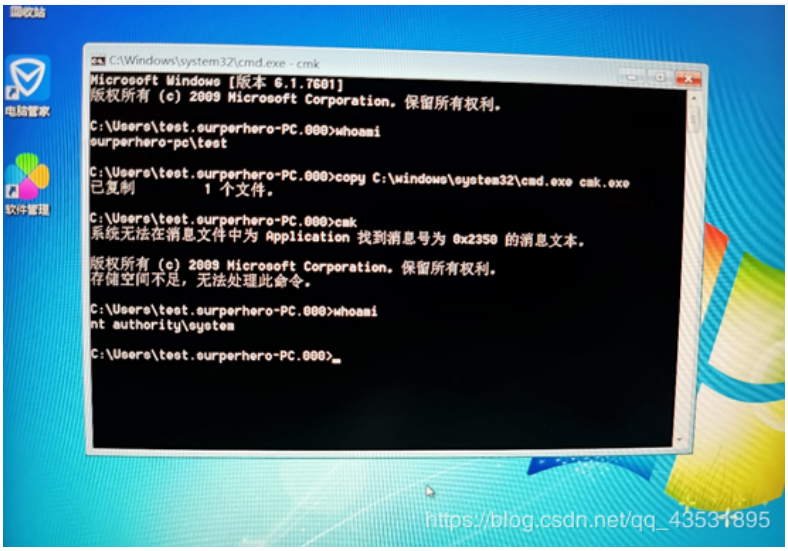
Kon-boot还具有提权功能，win7测试正常，win10我这个版本的似乎不行。

操作步骤为

登陆非管理员账户

打开cmd窗口，输入以下命令

copy c:\windows\system32\cmd.exe cmk.exe
cmk

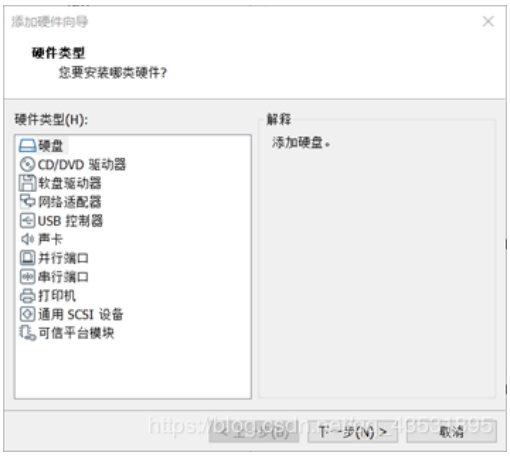


附：VMware虚拟机设置U盘启动方法

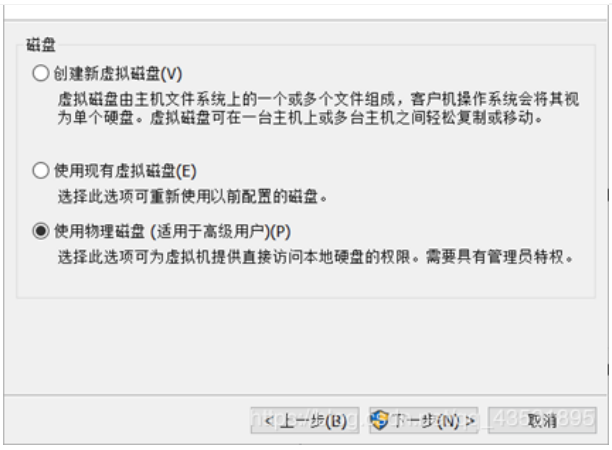
VMware虚拟机要使用U盘启动，必须先将U盘作为新加硬盘加入虚拟机

打开虚拟机设置，点击添加

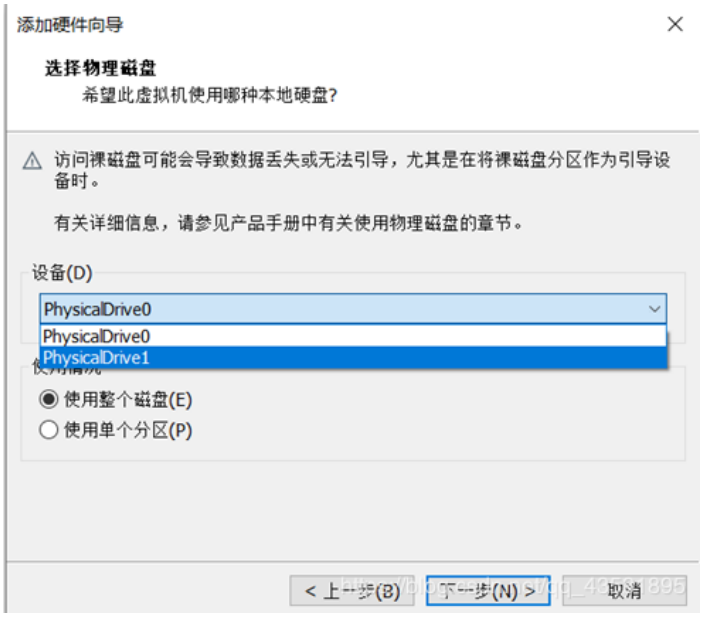
然后添加硬盘



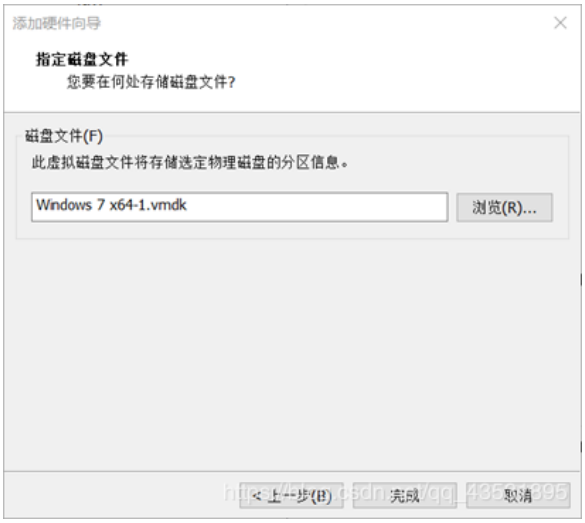
选择使用物理硬盘



选择设备，应该是下拉菜单的最后一个



默认，点击完成即可



之后进入BIOS选择U盘启动即可。

来自： 翱翔的真爱> 《待分类》

类似文章

- 间谍往事：电视里的那些密探谍报究竟如何...
- 小学语文：修辞手法运用口诀，寒假掌握扎...
- 直系亲属去世后必知的六大禁忌
- 大多数职场人，什么时候适合离职？从这3个...

精选文章

- 11个遇事有水平的处理方法
- 【民间秘方】神效慢性咽喉炎秘方—治愈患者...
- 酥鱼
- 最大的天敌

人人都是事后诸葛亮：批判性思维、决策与... 国外肖像铅笔画:我们不能拒绝美女的魔力

掌握五个自媒体创作技巧，赚钱与个人品牌... 2014年中国城市排名27强

发表评论： 评论公约