windows密码绕过工具



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

名称	修改日期
📙 kon-bootCD	2018/2/3 23:01
📙 kon-bootFLOPPY	2018/2/3 23:01
📙 kon-bootUSB	2020/3/25 15:02
3rd_party_licenses.txt	2017/12/10 0:53
📄 eula.txt	2018/2/3 23:01
INSTALL_GUIDE	2018/2/3 23:01
🗔 KonBootInstaller.exe	2018/2/3 23:01

https://blog.csdn.net/gg_43531895

ſ

我的图书馆

留言交流

搜文章 找馆友

The second states of the seco	千万人在用的知识管理与分享平台		
名称	修改日期		
📜 EFI	2018/2/3 23:01		
USBFILES	2018/2/3 23:01		
auto.ps1	2018/2/3 23:01		
COPYING	2000/12/19 12:47		
grubinst.exe	2008/1/2 5:53		

 README.txt
 2013/1/3 19:52

 temp_file.txt
 2020/3/25 15:02

 USB_INSTALL.vbs
 2015/8/4 23:47

 USB_INSTALL_DIFF.vbs
 2015/8/4 23:47

 usb_install_RUNASADMIN.bat
 2012/9/5 11:36

 usb_install2_NEEDADMIN.bat
 2012/9/5 11:36

https://blog.csdn.net/qq_43531895

接下来应该会出现下图,让你确认只有这一个USB存储设备。





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

倌

个人图书馆

360doc.com

我的图书馆

搜文章 找馆友

然后在Boot下将启动首选项设置为U盘启动, Boot菜单如图

千万人在用的知识管理与分享平台



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

馆

我的图书馆

搜文章 找馆友





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。



我的图书馆

搜文章 找馆友



个人图书馆 千万人在用的知识管理与分享平台

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)

BOOT Hanag	Providence Backhar
Done normally Uindows Boot Manager EFI UMware Uirtual SCSI Hard Drive (0.0) EFI UMware Uirtual SMIA CORON Drive (1.0) EFI Internal Shell (Unsupported option) EFI Unternal Shell (Unsupported Drive (1.0)	Beo Lee Falls: Pc: Root (0x0//Pc:1 (0x15,0x θ) /Pc1 (0x0,0x0) /Scsi (0x1 ,0x0)
Enter setup Reset the system Shut down the system	
11=Hove Highlight <enter>=Select E</enter>	htry

用上下键选中目标后回车即可进入kon-boot界面

我的图书馆

搜文章 找馆友



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

官

个人图书馆

我的图书馆

搜文章 找馆友

留言交流

 Image: Non-Mood
 Image: Nood
 Image: Non-Mood
 Imag

千万人在用的知识管理与分享平台

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。

Information Configuration Sec	urity Boot Exit	
Administrator Password User Password HDD Password Set Administrator Password Set Hard Disk Passwords	Not Set Not Set Not Set	Er [H Se [I] Se
Intel Platform Trust Technology Clear Intel PTT Key Fintel SGX	[Enabled] [Enter]	
Secure Boot Secure Boot Status Platform Mode Secure Boot Mode Reset to Setup Mode Restore Factory Keys	[Enabled] Enabled User Mode Standard [Enter] [Enter]	
	https://blog.code.pot/co.	42521805

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

喧

我的图书馆

搜文章 找馆友



个人图书馆 千万人在用的知识管理与分享平台

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







选择使用物理硬盘

1

个人图书馆 千万人在用的知识管理与分享平台 360doc.com	我的图书馆	搜文章 找馆友	留言交流
磁盘 创建新虚拟磁盘(V) 虚拟磁盘由主机文件系统上的一个或多个文件组成, 客户机操作系统会将其视 为单个硬盘。虚拟磁盘可在一台主机上或多台主机之间轻松复制或移动。 使用现有虚拟磁盘(E) 选择此选项可重新使用以前配置的磁盘。 使用物理磁盘(适用于高级用户)(P) 选择此选项可为虚拟机提供直接访问本地硬盘的权限。需要具有管理员特权。 			
○<(上+/步(B)) ◎ ホ+歩(N) > 483戦術895			
选择设备,应该是下拉菜单的最后一个			
添加硬件向导	×		
选择物理磁盘 希望此虚拟机使用哪种本地硬盘?			
▲ Gerie Gerie Gerie Gerie Gerie Gerie Approximation of the constant o			
< 上步(B) 下步(N) > 取	消 895		
指定磁盘文件 您要在何处存储磁盘文件?			
磁盘文件(F) 此虚拟磁盘文件将存储选定物理磁盘的分区信息。 Windows 7 x64-1.vmdk 浏览(R)			
□ [マ□ <u>上</u> 4-歩(B) ↓ 5cln 完成/c(c) [485版清895]			
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

精选文章

酥鱼

最大的天敌

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…

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...

www.360doc.com/showweb/0/0/912421562.aspx#

信 个人图书馆 千万人在用的知识管理 360doc.com	与分享平台	我的图书馆	搜文章 找馆友	留言交流
人人都是事后诸葛亮:批判性思维、决策与…	国外肖像铅笔证	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		