linux下破解windows密码究极版Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/619/2021_2022_linux_E4_B8_8B_E7_A0_c103_619614.htm 如果你有光驱，如果你有进入BIOS的权限，那么请你不要继续看这篇文章了，去找一张WindowsXP光盘就可以了，想怎么搞，怎么搞。 我这里要谈的问题是针对公司办公电脑的。公司IT部门跟普通职员永远是一对矛盾。IT部门应公司领导要求，或者自己管理方便，总是想尽办法让你拥有尽量少的权限。光驱，软驱就别想用了；BIOS密码是不会告诉你的（当然大多数情况下，这个不是问题）；C盘一定是NTFS格式的，boot.ini你就别去碰了，没有希望的，C盘有没有写的权限还需要看IT部同事们的心情呢；封USB一般分两种：物理端口贴封条，那叫人治，系统设置卡权限叫法制，相对来说前者比较阴险；用域控制器统一管理权限；还会用各种组策略卡你各种应用程序执行权限的…… 出于对自由的渴望，我们是绝对不会认输滴…… 前段时间我写过一篇John/bkhive/samdump，在Linux下破解SAM密的文章，是我的一个成功的案例，但是这不会绝对有用，因为如果BT的IT哥们把管理员密码设得足够复杂和长，那么就没辙了。这不，我换工作到新公司后就碰到了。让John帮我辛苦的算了1个月后，我决定放弃使用这种方法了 随便google一下，你就会发现windowsxp提升权限的方法N多，但是大多数是无效的，而铺天盖地的文章也只是不负责任的抄来抄去： 1.最著名的删除SAM文件，正常情况下你是没有办法动这个文件的。当你化大力气删掉这个文件后，会发现系统会崩溃。汗一下吧… 2.进入带命令行的安全模式，执

行net user admin 123 /add 类似的命令。sorry， 首先，普通用户要进入安全模式就是管理员的话，微软就别混那么多年了；其次，普通用户要能添加用户，再让他变成管理员的话，微软照样不用混了。汗第二下吧… 3.运行各种能探测windows密码的rootkit工具。又是一个鸡生蛋，蛋生鸡的问题。能成功运行这些工具的前提一般是你有管理员权限；要是有管理员权限，你TMD还需要这个？汗第三下吧… 4.写个bat文件，上书一下代码： net user admin 123 /add net localgroup administrators admin /add 代替logon.scr， magnify.exe等系统程序。 这个有点靠普，但是执行起来也有难度。一来，windows对这些文件是保护的，你没有办法修改，删除，或者重命名，即使你把硬盘拆下来放到另外一台windows的机器上也一样。但是本文的方法是基于这个的。 声明一下，这不是我独创的，思想方法来源于互联网，我只是通过实践证明了它的可行性，让我们在公司上班的自由斗士减少弯路而已。 好了，开始吧： 1. 准备好用户添加脚本。用写字板写下如下内容，并将文件名改成magnify.bat @net user admin /del @net user young001 123456 /add @net localgroup administrators young001 /add @exit 上述第一行会把admin用户删除，避免如果它存在影响后面两行的执行，如果不存在也不会影响后面两行的执行；第二行添加名为admin的帐户，密码设为123456；第三行将admin帐户加入到administrators用户组下；第四行退出 2. 将文件magnify.bat转化为exe格式。请你不要直接改后缀名，那样不能运行的。有一个工具叫bat2exe，可以转化：bat2exe 里面有，两个文件，bat2com.exe和com2exe.exe文件。分别用下面命令： bat2com magnify.bat //生成magnify.com文

件 com2exe magnify.com //生成magnify.exe文件 bat2exe工具是一个16位程序。如果上面连接无法下载，请google之 3.替换文件：将上面生成的magnify.exe文件替换C：\WINDOWS\systen32\magnify.exe文件。其实这个是放大镜程序，替换前，请确保先将原始magnify.exe备份好，以便用完后能够替换回去，linux认证，加入收藏！否则以后你的放大镜程序就用不了了。 这个是这里最难的部分。再次重申，如果你有光驱，软驱，USB，BIOS等资源，请你用windowsXP光盘这个方便的方法，别走远路了。我是将硬盘拆下，放到Linux系统下替换的（顺便用到NTFS3g程序使得Linux对NTFS可写，这里用到的Linux下Mount windows分区，修改文件等知识不在本篇主题以内，就不讨论了。如果你需要，可以问我）。你也可以用其他办法，但是硬盘是拆定了，要不然没辙；另外一个系统确定别用WindowXP，因为这样不会成功。 4.运行magnify.exe.启动WindowsXP到登录界面，按Ctrl U，弹出辅助工具对话框，上面有两个程序可选，放大镜程序和屏幕键盘程序。选放大镜，点击运行。然后你就可以用帐户admin密码123456登录。 恭喜，系统就是你的了。记得将原来的放大镜程序替换回去 这里只是我的成功方法，但是过程一定不是唯一的。比如替代程序不一定就是放大镜程序，你也可以用屏幕键盘程序。文件替换的过程就更加天马行空了，完全在于你的创造力了。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com