黑客入侵Linux操作系统实例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_ti2020/616/2021_2022__E9_BB_91_E5_AE_A2_E5_85_A5_E4_c103_616633.htm 我发现了一个网站，于是常规入侵。很好，它的FINGER开着，于是我编了一个SHELL，aaa帐号试到zzz(by the way，这是我发现的一个网上规律，那就是帐号的长度与口令的强度成正比，如果一个帐号只有两三位长，那它的口令一般也很简单，反之亦然，故且称之为若氏定理吧)，结果一个帐号也不存在，我没有再试它的帐号。因为我被它开的端口吸引住了，它开着WWW，我就不信它不出错。一连拿了五种CGI和WWW扫描器总计扫了三四百种常见错误它几乎都不存在还是看看root的信息吧： finger root@xxx.xxx.xxx Login name: root In real life: system PRIVILEGED account Directory: / Shell: /bin/sh Last login Fri Jul 28 09:21 on ttyp0 from 202.xx.xx.xx No Plan. root经常来，那个202.xx.xx.xx就是他用的工作linux认证更多详细资料站了，从那会不会看到点东西呢? net view \202.xx.xx.xx Shared resources at \202.xx.xx.xx Sharename Type Comment x x 我的公文包 The command was completed successfully. 在上网的机器上开着WINDOWS的“ 文件和打印机共享 ”的服务，是很多人容易掉以轻心的，这个root没有例外。如果它的C盘共享了而且可写那就好了，但那是做梦，现在开了共享的目录没有一个是根目录，连D驱的都没有。别着急，慢慢来。x掉的那些文件夹都没用，不能写，里面尽是些英文原著，这个root还挺行的。“ 我的公文包 ”吸引了我的注意，这是一个用于将不同的机器上的资料进行同步的工具，很显然这个root要经常

更新主机上的主页，有时候在自己的机器上编，有时候在主机上编……所以很重要的一点：“ 我的公文包 ”的共享一般都是可写的! 那我再进去看看。 gt.i: gt.temp.txt 不错，确实可写。 gt.dir/od/p 看看都有些什么…… 倒数第二排那个是什么? “ X月工作计划.doc ”!就是它了，既然是计划就不可能写完了就丢一边，它肯定会再次打开它的至少下个月写计划时要COPY一下:-gt.copy hookdump.* i: 补充一点：上传前先编好它的hookdump.ini文件，置为隐藏方式运行，不然root一运行屏幕上蹦出一大窗口可就……。 然后再在自己的机器上编一个同名的BAT文件：X月工作计划.BAT gt.copy X月工作计划.bat i: gt.attrib h X月工作计划.doc &gt.attrib h X月工作计划.bat 这样，root的 “ 公文包 ” 里只剩下一个和原来一模一样的WORD图标，他做梦也没想到这已变成了一个BAT文件。 然后可以喘口气了，让我们静静的等…… 几天后，我进入这个工作站，取下记录下来的击键记录，找出root的口令，进入主机。 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