伪装Linux假象加强自身安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E4_BC_AA_E8_A3_85Linu_c103_645585.htm 通过伪装Linux系统，给黑客设置系统假象，可以加大黑客对系统的分析难度，引诱他们步入歧途，从而进一步提高计算机系统的安全性。下面以Red Hat Linux为例，针对几种黑客常用的途径介绍一些常用的Linux系统伪装的方法。 针对HTTP服务 通过分析Web服务器的类型，大致可以推测出操作系统的类型，比如，Windows使用IIS来提供HTTP服务，而Linux中最常见的是Apache。 默认的Apache配置里没有任何信息保护机制，并且允许目录浏览。通过目录浏览，通常可以获得类似“ Apache/1.3.27 Server at apache.linuxforum.net Port 80 ”或“ Apache/2.0.49 (Unix) PHP/4.3.8 ”的信息。 通过修改配置文件中的ServerTokens参数，可以将Apache的相关信息隐藏起来。但是，Red Hat Linux运行的Apache是编译好的程序，提示信息被编译在程序里，要隐藏这些信息需要修改Apache的源代码，然后，重新编译安装程序，以实现替换里面的提示内容。 以Apache 2.0.50为例，编辑ap_release.h文件，修改“ #define AP_SERVER_BASEPRODUCT \ Apache\ ”为“ #define AP_SERVER_BASEPRODUCT \Microsoft-IIS/5.0\ ”。编辑 os/unix/os.h文件，修改“ #define PLATFORM \Unix\ ”为“ #define PLATFORM \Win32\ ”。修改完毕后，重新编译、安装Apache。 Apache安装完成后，修改httpd.conf配置文件，将“ ServerTokens Full ”改为“ ServerTokens Prod ”；将“ ServerSignature On ”改为“ ServerSignature Off ”，然后存盘

退出。重新启动Apache后，用工具进行扫描，发现提示信息中已经显示操作系统为Windows。 针对FTP服务 通过FTP服务，也可以推测操作系统的类型，比如，Windows下的FTP服务多是Serv-U，而Linux下常用vsftpd、proftpd和pureftpd等软件。 以proftpd为例，修改配置文件proftpd.conf，添加如下内容：ServerIdent on \Serv-U FTP Server v5.0 for WinSock ready...\ 存盘退出后，重新启动proftpd服务，登录到修改了提示信息的FTP服务器进行测试： C:\\ftp 192.168.0.1 Connected to 192.168.0.1. 220 Serv-U FTP Server v5.0 for WinSock ready... User (192.168.0.1:(none)): 331 Password required for (none). Password: 530 Login incorrect. Login failed. ftp 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