

深入分析Linux操作系统深度安全加固（3）PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/144/2021\\_2022\\_\\_E6\\_B7\\_B1\\_E5\\_85\\_A5\\_E5\\_88\\_86\\_E6\\_c103\\_144451.htm](https://www.100test.com/kao_ti2020/144/2021_2022__E6_B7_B1_E5_85_A5_E5_88_86_E6_c103_144451.htm) 5. Banner 伪装入侵者通常通过操作系统，服务及应用程序版本来攻击，漏洞列表和攻击程序也是按此来分类，所以我们有必要作点手脚来加大入侵的难度。更改 /etc/issue，因为 reboot 后重新加载，所以编辑 /ect/rc.d/rc.local：# This will overwrite /etc/issue at every boot. So，make any changes you # want to make to /etc/issue here or you will lose them when you reboot. #echo "" > /etc/issue #echo "\$R" >> /etc/issue #echo "Kernel \$(uname -r) on \$a \$(uname -m)" >> /etc/issue # #cp -f /etc/issue /etc/issue.net #echo >> /etc/issue Apache 不回显版本，apache 的配置文件，找到 ServerTokens 和 ServerSignature 两个 directive，修改默认属性：#ServerTokens Full ServerTokens Prod 修改 uname，拿出 uname.c 的源码，找到如下行：print\_element (PRINT\_SYSNAME，name.sysname).//操作系统名如 linux print\_element (PRINT\_NODENAME，name.nodename).//主机名 print\_element (PRINT\_RELEASE，name.release).//发行版本，如：2.4.20-18 print\_element (PRINT\_VERSION，name.version).// print\_element (PRINT\_MACHINE，name.machine).//机器类型，如i686 print\_element (PRINT\_PROCESSOR，processor).//处理器类型可以修改为：print\_element (PRINT\_SYSNAME，"HP-UX"). .....编译后替换 /bin/uname 其他服务及程序的修改可以查看其配置文件或者源码不要改太多，否则会给系统管理带来太麻烦。 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](http://www.100test.com)