

Linux网络安全之经验谈(5) 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\\_Linux\\_E7\\_BD\\_91\\_E7\\_BB\\_c103\\_645710.htm](https://www.100test.com/kao_ti2020/645/2021_2022_Linux_E7_BD_91_E7_BB_c103_645710.htm) 关于日志 所有的日志都在/var/log下（仅对linux系统而言），默认情况下linux的日志就已经很强大，但除ftp外。因此我们可以通过修改/etc/ftpaccess 或者/etc/inetd.conf，来保证每一个ftp连接日志都能够纪录下来。下面是一个修改inetd.conf的例子，假如有下一行：`ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -L -i -o`  
注释：`-l` 每一个ftp连接都写到syslog `-L` 纪录用户的每一个命令 `-i` 文件received,纪录到xferlog `-o` 文件transmitted,记录到xferlog 不过你也不要太相信日志，因为绝大部分黑客都有“擦脚印”的“好”习惯！如果你不放心，最好安装一个Sniffer吧。关于TCP\_WRAPPERS默认的，Redhat Linux允许所有的请求，这是很危险的。如果用TCP\_WRAPPERS来增强我们站点的安全性简直是举手之劳，你可以将禁止所有的请求放入“ALL: ALL”到/etc/hosts.deny中，然后放那些明确允许的请求到/etc/hosts.allow中，如: sshd:

`192.168.1.10/255.255.255.0 gate.openarch.com` 对IP地址192.168.1.10和主机名gate.openarch.com，允许通过ssh连接。配置完了之后，用tcpdchk检查，你可以直接执行：`tcpdchk`。在这里，`tcpchk`是TCP\_Wrapper配置检查工具，它检查你的tcp wrapper配置并报告所有发现的潜在/存在的问题。关于补丁 你应该经常到你所安装的Linux系统发行商的主页上去找最新的补丁。例如：对于Redhat系统而言可以在

：<http://www.redhat.com/corp/support/errata/>上找到补丁。幸运

的是，在Redhat6.1以后的版本带有一个自动升级工具up2date，它能自动测定哪些rpm包需要升级，然后自动从Redhat的站点下载并完成安装。这对某些懒惰的管理人员来说，是个省精神的福音。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)