加强安全:看清黑客怎样入侵linux PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/462/2021_2022__E5_8A_A0_E5_BC_BA_E5_AE_89_E5_c103_462220.htm 此文的目的不在于教人入侵，而是为了提高自身的技术和加强网络管理员的安全防范意识。仅此而已!粗心大意的网络管理员应该明白：由于你们一个小小的操作失误可能会导致整个网络全面沦陷!本文主要是围绕LPD：网络打印服务的攻击而进行的。 首先确定目标，假设是：www.XXX.com 先让俺看看是不是连得上：以下是引用片段： C:\ping www.XXX.com Pinging www.XXX.com[202.106.184.200] with 32 bytes of data: Reply from 202.106.184.200: bytes=32 time=541ms TTL=244 Reply from 202.106.184.200: bytes=32 time=620ms TTL=244 Reply from 202.106.184.200: bytes=32 time=651ms TTL=244 Reply from 202.106.184.200: bytes=32 time=511ms TTL=244 Ping statistics for 202.106.184.200: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 511ms, Maximum = 651ms, Average = 580ms 嘻嘻不但连得上，速度还不错…… 先telnet看看banner： C:\>telnet www.XXX.com 遗失对主机的连接。 再试试ftp,以下是引用片段：C:\>ftp www.XXX.com Connected to www.fbi.gov.tw. 220 XXX-www FTP server (Version wu-2.6.1(1) Wed Aug 9 05:54:50 EDT 2000) ready. User (www.XXX.com:(none)): wu-2.6.1看来有点眉目了。这台机器像是RedHat7.0!首先必须确认一下，连上俺的跳板: 以下是引用片段： C:\>telnet xxx.xxx.xxx.xxx Red Hat Linux release 7.0 (Guinness) Kernel 2.2.16-22smp on an i686 login: fetdog

Password: bash-2.04$ 拿nmap扫描器，看看其中的奥妙~~~以下是引用片段： bash-2.04$nmap -sT -O www.XXX.com Starting nmap V. 2.54BETA7 (www.insecure.org/nmap/) WARNING! The following files exist and are readable: /usr/local/sha -services and ./nmap-services. I am choosing /usr/local/share/nmap/ s for security reasons. set NMAPDIR=. to give priority to files in irectory Interesting ports on (www.XXX.com): (The 1520 ports scanned but not shown below are in state: closed) Port State Service 25/tcp open smtp 79/tcp open finger 80/tcp open http 111/tcp open sunrpc 113/tcp open auth 443/tcp open https 513/tcp open login 514/tcp open shell 515/tcp open printer 587/tcp open submission 1024/tcp open kdm TCP Sequence Prediction: Class=random positive increments Difficulty=3247917 (Good luck!) Remote operating system guess: Linux 2.1.122 - 2.2.16 Nmap run completed -- 1 IP address (1 host up) scanned in 9 seconds 打开的端口还挺多，这意味着入侵的可能性增加。79/tcp open finger ，先看看这个，不过linux没有finger用户列表这个漏洞。