深入分析Linux操作系统深度安全加固（4） 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_144453.htm 6. Iptales 防火墙规则假设我们的服务器 server1 运行 apache，sshd (sshd 可以不运行在标准端口，配置文件中能修改)eth0 网卡接 Internet，eth1 连接 LAN，管理员在家中拨号登陆到 server2 (其私用网络 IP 为 192.168.0.12)，再登陆 server1[roor@ayazero root]# iptables -A INPUT -i eth1 -s 192.168.0.12 -p tcp --dport 22 -j ACCEPT为防止 IP spoofing 的可能，还可以绑定 server2 的网卡地址：sh-2.05b# iptables -A INPUT -i eth1 -s 192.168.0.12 --mac-source 01:68:4B:91:CC:B7 -p tcp --dport 22 -j ACCEPT不过好像也很少有入侵者能够做到这种地步，而且没什么利用的价值。 [root@ayazero root]# iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT [root@ayazero root]# iptables -A INPUT -m state --state ESTABLISHED，RELATED -j ACCEPT [root@ayazero root]# iptables -A INPUT -j DROP 对攻击有所了解的人都知道“ 端口重定向 反向管道 ”的美妙结合来穿越防火墙的例子吧这种技巧已经运用太广，而危害很大为了对抗这种难以防御的攻击，我们必须以牺牲一定的易用性为代价 [root@ayazero root]# iptables -A OUTPUT -o eth0 -p tcp --syn -j DROP以上规则将阻止由内而外的 TCP 主动连接另外，用 tftp 或其他客户端反向攫取文件的攻击行为也很普遍，由于 tftp 以及其他一些工具依赖 UDP，所以现在要把它彻底抹煞掉[root@ayazero root]# iptables -A OUTPUT -o eth0 -p udp -j DROPPS: 在更新系统和调试网络时需要把这两条规则临时去

掉因为入侵的本质就是通过文本或图形界面在标准或非标准端口得到目标操作系统的 shell，所以，这不仅能阻止反向管道本身，还能免疫很多入侵技巧不过对一般的系统管理员而言，这太苛刻了！iptables 的一些攻击对策: Syn-flood protection: [root@ayazero foo]# iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT Furtive port scanner: [root@ayazero foo]# iptables -A FORWARD -p tcp --tcp-flags SYN，ACK，FIN，RST RST -m limit --limit 1/s -j ACCEPT Ping of death: [root@ayazero foo]# iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT此外，iptables 还能配置出让一些扫描行为比如 nmap 失效的规则，应当注意：防火墙不是万能的，当一个攻击者足够疯狂时，不要指望你的防火墙能抵挡得住 DDoS 的洪水。关于 iptables 得更多细节，请参阅 Rusty Russell 的 Packet Filtering HOWTO。 7. 完整性校验 tripwire 是一个比较有名的工具，它能帮你判断出一些重要系统文件是否被修改过现在的 Linux 发行版中一般都带有他的开源版本，在默认的校验对象配置文件中加入一些敏感文件就可以使用RPM MD5 校验: [root@ayazero rpm]# rpm -V用 "man rpm" 查看命令帮助，"-V" 参数用于 MD5 校验，注意要把 rpm 校验产生的二进制数据文件作一个硬备份，以防止其本身被修改。 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