用Shell写DEAMON后台来控制安全访问的方法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/267/2021_2022__E7_94_A8Shell_E5_86_c103_267171.htm 我的控制访问比较特殊，考虑到远程登陆点并非固定，所以无法设定固定IP通过SSH登陆服务器。这样N多IP会通过黑客软件试图破解您的用户名和密码（基本都是穷举，不怕一万只怕万一，因此我写了这个后台脚本）。 安全：利用/etc/hosts.deny、/etc/hosts.allow来做tcp wrapper控制访问，配合iptables作进一步过滤。 crontab最短执行周期是每隔1分钟执行一次，而以下这段代码的最短执行周期可以自定义（最短1秒） 脚本名:sshd_monitor #!/bin/sh while true #使用while true来做循环,这样当脚本后台执行的时候总是会根据sleep时间的长短来执行任务 do cat /var/log/secure* |awk {if($6=="Invalid")print $10} |sed s/::ffff://g |sort -n |uniq -c |awk {if($1>=5)print $2} >/root/lawless_ip #在secure日志中，获取登陆失败大于5次的ip并输入到lawless_ip文件中 row=`cat /root/lawless_ip|wc -l` #记录lawless_ip文件中的ip记录条数 a=0 for z in `seq 1 $row` #从第一个ip开始写规则到lawless_ip_deny这个临时文件中，起结果会类似 ALL:123.123.123.123 …… do a=$[$a 1] row_ip=`cat /root/lawless_ip |sed -n -e ""$a"p"` echo -e "ALL:$row_ip" >> /root/lawless_ip_deny done cat /root/lawless_ip_deny > /etc/hosts.deny #然后将lawless_ip_deny文件中的内容写入到hosts.deny。 rm /root/lawless_ip_deny #删除该临时文件 sleep 10 #每隔10秒执行while操作 done 为防止自己登陆失败超过5次被禁止，需要在/etc/hosts.allow中加入自己本机或许可某个IP总是能够登陆的匹配规则如: ALL:192.168.10.12

。记住，一般allow的优先级总比deny高。此外，在/etc/rc.local加句sh /dir/sshd_monitor &amp.，保证每次启动服务器时都能后台运行该脚本。 以上方法只是抛砖引玉，这样的deamon可以写成监控ftp、http、进程等各种需求，相当实用。 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