巧用Recent模块加固Linux安全Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_B7_A7_E7_94_A8Rece_c103_644875.htm 众所周知，Linux可以通过编写iptables规则对进出Linux主机的数据包进行过滤等操作，在一定程度上可以提升Linux主机的安全性，在新版本内核中，新增了recent模块，该模块可以根据源地址、目的地址统计最近一段时间内经过本机的数据包的情况，并根据相应的规则作出相应的决策，详见 ：http://snowman.net/projects/ipt_recent/ 1、通过recent模块可以防止穷举猜测Linux主机用户口令，通常可以通过iptables限制只允许某些网段和主机连接Linux机器的 22/TCP端口，如果管理员IP地址经常变化，此时iptables就很难适用这样的环境了。通过使用recent模块，使用下面这两条规则即可解决问题 ： -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --0update --seconds 60 --hitcount 4 --name SSH --rsource -j DROP -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name SSH --rsource -j ACCEPT 应用该规则后，如果某IP地址在一分钟之内对Linux主机22/TCP端口新发起的连接超过4次，之后的新发起的连接将被丢弃。 2、通过recent模块可以防止端口扫描。 -A INPUT -m recent --0update --seconds 60 --hitcount 20 --name PORTSCAN --rsource -j DROP -A INPUT -m recent --set --name PORTSCAN --rsource -j DROP 应用该规则后，如果某个IP地址对非Linux主机允许的端口发起连接，并且一分钟内超过20次，则系统将中断该主机与本机的连接。 详细配置如下： *filter :INPUT DROP [0:0]

:FORWARD ACCEPT [0:0] :OUTPUT ACCEPT [458:123843] -A INPUT -i lo -j ACCEPT -A INPUT -i tap -j ACCEPT -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT -A INPUT -m recent --0update --seconds 60 --hitcount 20 --name PORTSCAN --rsource -j DROP -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --0update --seconds 60 --hitcount 4 --name SSH --rsource -j DROP -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name SSH --rsource -j ACCEPT -A INPUT -p udp -m udp --dport 53 -j ACCEPT -A INPUT -p tcp -m tcp --dport 53 -m state --state NEW -j ACCEPT -A INPUT -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT -A INPUT -p tcp -m tcp --dport 443 -m state --state NEW -j ACCEPT -A INPUT -m recent --set --name PORTSCAN --rsource -j DROP COMMIT 以上配置说明，本机开放可供服务的端口有22/TCP（有连接频率限制）,53/TCP/UDP, 80/TCP, 443/TCP，所有发往本机的其他ip报文则认为是端口扫描，如果一分钟之内超过20次，则封禁该主机，攻击停止一分钟以上自动解封。 在这只是取个抛砖引玉的作用，通过recent模块还可以实现很多更复杂的功能，例如：22/TCP端口对所有主机都是关闭的，通过顺序访问23/TCP 24/TCP 25/TCP之后，22/TCP端口就对你一个IP地址开放等等。 