分类防范对Linux的DoS攻击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_88_86_E7_B1_BB_E9_98_B2_E8_c103_644866.htm 由于拒绝服务攻击工具的泛滥，及所针对的协议层的缺陷短时无法改变的事实，拒绝服务攻击也就成为流传广泛、极难防范的一种攻击方式。虽然到目前为止，没有一个绝对的方法可以制止这类攻击.但对于不同的攻击方式，还是有一些解决方法的。本文以Redhat Linux 9.0为例，介绍如何分类防范DoS. Linux服务器的两种守护进程 1.stand-alone模式 stand-alone方式是Unix传统的C/S模式的访问模式。服务器监听(Listen)在一个特点的端口上等待客户端的联机。如果客户端产生一个连接请求，守护进程就创建(Fork)一个子服务器响应这个连接，而主服务器继续监听，以保持多个子服务器池等待下一个客户端请求。 工作在stand-alone模式下的网络服务有route、gated.大家比较熟悉的Web服务器是Apache和邮件服务器Sendmail.在Apache这种负载很大的服务器上，预先创子服务器可以提高客户的服务速度。 在Linux系统中通过stand-alone工作模式启动的服务由/etc/rc.d/下面对应的运行级别当中的符号链接启动。 2.xinetd模式 从守护进程的概念可以看出，对于系统所要通过的每一种服务都必须运行一个监听某个端口连接所发生的守护进程，这通常意味着资源浪费。为了解决这个问题，Linux引进了“ 网络守护进程服务程序 ”的概念。 Redhat Linux 9.0使用的网络守护进程是xinetd(eXtended InterNET daemon)。和stand-alone模式相比，xinetd模式也称Internet Super-Server(超级服务器)。xinetd能够同时监听多个指定的端口，在接受

用户请求时能根据用户请求端口的不同，启动不同的网络服务进程来处理这些用户请求。我们可以把xinetd看成一个管理启动服务的管理服务器，它决定把一个客户请求交给哪个程序处理，然后启动相应的守护进程。 和stand-alone工作模式相比，系统不想要每一个网络服务进程都监听其服务端口，运行单个xinetd就可以同时监听所有服务端口，这样就降低了系统开销，保护了系统资源。但是对于访问量大、经常出现并发访问时，xinetd想要频繁启动对应的网络服务进程，反而会导致系统性能下降。 察看系统为Linux服务提供哪种模式方法，在Linux命令行下使用pstree命令，可以看到两种不同方式启动的网络服务。一般来说系统一些负载高的服务，如Sendmail、Apache服务是单独启动的，而其他服务类型都可以使用xinetd超级服务器管理，系统默认使用xinetd的服务可以分为如下几类： 标准互联网服务：telnet、ftp 信息服务：finger、netstat、systat RPC服务：rquotad、rstatd、rusersd、sprayd、walld BSD服务：comsat、exec、login、ntalk、shell、talk 内部服务：chargen、daytime、echo、servers、services time 安全服务：irc 其他服务：name、tftp、uucp 小提示：从原理上Apache、sendmail也可以使用xinetd模式启动，但是您需要硬件档次非常高的服务器。 针对xinetd模式的DoS防范 xinetd提供类似于inetd tcp_wrapper的功能，但是更加强大和安全，能有效防止DoS： 1.限制同时运行的进程数 通过设置instances选项设定同时运行的并发进程数。例如： instances=20 说明：当服务器被请求连接的进程数达到20个时，xinetd将停止接受多出部分的连接请求，直到请求连接数低于设定值为止。 2.限制一个IP地址的最大连接数 通过限制一

个主机的最大连接数来防止某个主机独占某个服务。例如：per_source=5 说明：单个IP地址的连接数是5个。 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