

构筑Unix系统内防火墙体系的多种方案 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_9E_84_E7_AD_91Unix_c103_144411.htm

近一段时间,某银行地市级分行计算机中心的某些服务器,如储蓄服务器、本地服务器多次出现了相同的奇怪现象:正常运行的计算机被意外关掉。经检查机器的各方面资源都没有明显的故障,而且相同配置的服务器也只是个别机器被关掉,最关键的是被关的机器上除了关机信息外没有其他报错信息。综合种种迹象确定,是市分行下属的某县支行机房中有人用telnet登录到市分行的服务器,进入一个菜单用户后,执行了菜单中的关机选项而关掉了正在运行的机器。通过这件事例,使人警觉到利用远程计算机进行高科技作案的潜在危险。目前银行系统的计算机网络发展迅猛,由于全省乃至全国通存通兑的需要,地市级分行的计算机系统对上要与省分行的计算机网络相连,对下连通了全市所辖的数十家县市工行或办事处的计算机.又由于代理业务和电子商务的需要,银行内部网络必须与越来越多的被代理企事业单位的计算机相连。这样一个庞大的网络,要防范“黑客”的偷袭确实有一定的困难。为了使Unix服务器或前置机能安全正常地运行,必须及时地根据业务的不同应用和需求,有针对性地构筑Unix系统内的防火墙体系,对远程登录和远程数据传输进行过滤,从而实现Unix防火墙的作用,同时能保障合法计算机远程业务操作的正常进行。下面把多种防火墙体系的具体实现方案介绍给读者。方案一 禁止其他任何计算机向本机的远程登录和远程数据传输。设置方法 进入超级用户,用vi打开/etc/inetd.conf文件,用"# "字封闭ftp、telnet、login、exec打头的四行,然后

执行/etc/inetd命令,即可生效。特点网络中其他计算机都无法远程登录和传输数据到本机,但本机却可以登录到其他计算机,也可向其他计算机收发数据。对本机来说,远程登录和数据传输变为单向操作,虽然其设置非常简单,但它的应用范围极为有限。方案二 禁止其他任何计算机向本机的远程登录,允许其他计算机向本机部分用户的远程传输数据。设置方法以允许用ftp到本机的普通用户而禁止用ftp到超级用户为例。(1)进入超级用户,用vi打开/etc/inetd.conf文件,用“#”字封闭telnet、login、exec打头的三行,并放开ftp,然后执行/etc/inetd命令。(2)用vi修改/etc/passwd文件,把第一行 root:x:0:1:Superuser:/: 改为 root:x:0:1:Superuser:/:/bin/shcheck (3)用vi创建/etc/shcheck文件,内容如下 /bin/sh /etc/profile /bin/sh /.profile /bin/sh - sh

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