对Linux服务器四种级别攻击的概述 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022__E5_AF_B9Linux_E6_9C_c103_145016.htm 随着Linux企业应用的扩展，有大量的网络服务器使用Linux操作系统。Linux服务器的安全性能受到越来越多的关注，这里根据Linux服务器受到攻击的深度以级别形式列出，并提出不同的解决方案。 对Linux服务器攻击的定义是：攻击是一种旨在妨碍、损害、削弱、破坏Linux服务器安全的未授权行为。攻击的范围可以从服务拒绝直至完全危害和破坏Linux服务器。对Linux服务器攻击有许多种类,本文从攻击深度的角度说明，我们把攻击分为四级。 攻击级别一：服务拒绝攻击（DoS） 由于DoS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，DoS也就成为了流传最广、最难防范的攻击方式。 服务拒绝攻击包括分布式拒绝服务攻击、反射式分布拒绝服务攻击、DNS分布拒绝服务攻击、FTP攻击等。大多数服务拒绝攻击导致相对低级的危险，即便是那些可能导致系统重启的攻击也仅仅是暂时性的问题。这类攻击在很大程度上不同于那些想获取网络控制的攻击，一般不会对数据安全有影响，但是服务拒绝攻击会持续很长一段时间，非常难缠。 到目前为止，没有一个绝对的方法可以制止这类攻击。但这并不表明我们就应束手就擒，除了强调个人主机加强保护不被利用的重要性外，加强对服务器的管理是非常重要的一环。一定要安装验证软件和过滤功能，检验该报文的源地址的真实地址。另外对于几种服务拒绝可以采用以下措施：关闭不必要的服务、限制同时打开的Syn半连接数目、缩短Syn半连接的time out 时间、及

时更新系统补丁。 攻击级别二：本地用户获取了他们非授权的文件的读写权限 本地用户是指在本地网络的任一台机器上有口令、因而在某一驱动器上有一个目录的用户。本地用户获取到了他们非授权的文件的读写权限的问题是否构成危险很大程度上要看被访问文件的关键性。任何本地用户随意访问临时文件目录（/tmp）都具有危险性，它能够潜在地铺设一条通向下一级别攻击的路径。 级别二的主要攻击方法是：黑客诱骗合法用户告知其机密信息或执行任务，有时黑客会假装网络管理人员向用户发送邮件，要求用户给他系统升级的密码。 由本地用户启动的攻击几乎都是从远程登录开始。对于Linux服务器，最好的办法是将所有shell账号放置于一个单独的机器上，也就是说，只在一台或多台分配有shell访问的服务器上接受注册。这可以使日志管理、访问控制管理、释放协议和其他潜在的安全问题管理更容易些。还应该将存放用户CGI的系统区分出来。这些机器应该隔离在特定的网络区段，也就是说，根据网络的配置情况，它们应该被路由器或网络交换机包围。其拓扑结构应该确保硬件地址欺骗也不能超出这个区段。 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