Linux服务器的四种入侵级别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_ti2020/641/2021_2022_Linux_E6_9C_8D_E5_8A_c103_641395.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。 攻击级别三：远程用户获得特权文件的读写权限 第三级别的攻击能做到的不只是核实特定文件是否存在，而且还能读写这些文件。造成这种情况的原因是：Linux服务器配置中出现这样一些弱点：即远程用户无需有效账号就可以在服务器上执行有限数量的命令。 密码攻击法是第三级别中的主要攻击法，损坏密码是最常见的攻击方法。密码破解是用以描述在使用或不使用工具的情况下渗透网络、系统或资源以解锁用密码保护的资源的一个术语。用户常常忽略他们的密码，密码政策很难得到实施。黑客有多种

工具可以击败技术和社会所保护的密码。主要包括：字典攻击 (Dictionary attack)、混合攻击(Hybrid attack)、蛮力攻击(Brute force attack)。一旦黑客拥有了用户的密码，他就有很多用户的特权。密码猜想是指手工进入普通密码或通过编好程序的正本取得密码。一些用户选择简单的密码 如生日、纪念日和配偶名字，却并不遵循应使用字母、数字混合使用的规则。对黑客来说要猜出一串8个字生日数据不用花多长时间。 防范第三级别的攻击的最好的防卫方法便是严格控制进入特权，即使用有效的密码。 主要包括密码应当遵循字母、数字、大小写(因为Linux对大小写是有区分)混合使用的规则。使用象“ # ”或“ % ”或“ $ ”这样的特殊字符也会添加复杂性。例如采用"countbak"一词，在它后面添加“ #$ ”(countbak#$)，这样您就拥有了一个相当有效的密码。 攻击级别四：远程用户获得根权限 第四攻击级别是指那些决不应该发生的事发生了，这是致命的攻击。表示攻击者拥有Linux服务器的根、超级用户或管理员许可权，可以读、写并执行所有文件。换句话说，攻击者具有对Linux服务器的全部控制权，可以在任何时刻都能够完全关闭甚至毁灭此网络。 攻击级别四主要攻击形式是TCP/IP连续偷窃，被动通道听取和信息包拦截。TCP/IP连续偷窃，被动通道听取和信息包拦截，是为进入网络收集重要信息的方法，不像拒绝服务攻击，这些方法有更多类似偷窃的性质，比较隐蔽不易被发现。一次成功的TCP/IP攻击能让黑客阻拦两个团体之间的交易，提供中间人袭击的良好机会，然后黑客会在不被受害者注意的情况下控制一方或双方的交易。通过被动窃听，黑客会操纵和登记信息，把文件送达，也会从目标系统上所有可通过的通

道找到可通过的致命要害。黑客会寻找联机和密码的结合点，认出申请合法的通道。信息包拦截是指在目标系统约束一个活跃的听者程序以拦截和更改所有的或特别的信息的地址。信息可被改送到非法系统阅读，然后不加改变地送回给黑客。 TCP/IP连续偷窃实际就是网络嗅探，注意如果您确信有人接了嗅探器到自己的网络上，可以去找一些进行验证的工具。这种工具称为时域反射计量器(Time Domain Reflectometer，TDR)。TDR对电磁波的传播和变化进行测量。将一个TDR连接到网络上，能够检测到未授权的获取网络数据的设备。不过很多中小公司没有这种价格昂贵的工具。对于防范嗅探器的攻击最好的方法是： 1、安全的拓扑结构。嗅探器只能在当前网络段上进行数据捕获。这就意味着，将网络分段工作进行得越细，嗅探器能够收集的信息就越少。 2、会话加密。不用特别地担心数据被嗅探，而是要想办法使得嗅探器不认识嗅探到的数据。这种方法的优点是明显的：即使攻击者嗅探到了数据，这些数据对他也是没有用的。 特别提示： 应对攻击的反击措施 对于超过第二级别的攻击您就要特别注意了。因为它们可以不断的提升攻击级别，以渗透Linux服务器。此时，我们可以采取的反击措施有： 首先备份重要的企业关键数据。 改变系统中所有口令，通知用户找系统管理员得到新口令。 隔离该网络网段使攻击行为仅出现在一个小范围内。 允许行为继续进行。如有可能，不要急于把攻击者赶出系统，为下一步作准备。 记录所有行为，收集证据。这些证据包括：系统登录文件、应用登录文件、AAA(Authentication、Authorization、 Accounting，认证、授权、计费)登录文件，RADIUS(Remote Authentication Dial-In

User Service)登录，网络单元登录(Network Element Logs)、防火墙登录、HIDS(Host-base IDS，基于主机的入侵检测系统)事件、NIDS(网络入侵检测系统)事件、磁盘驱动器、隐含文件等。收集证据时要注意：在移动或拆卸任何设备之前都要拍照.在调查中要遵循两人法则，在信息收集中要至少有两个人，以防止篡改信息.应记录所采取的所有步骤以及对配置设置的任何改变，要把这些记录保存在安全的地方。检查系统所有目录的存取许可，检测Permslist是否被修改过。 进行各种尝试(使用网络的不同部分)以识别出攻击源。 为了使用法律武器打击犯罪行为，必须保留证据，而形成证据需要时间。为了做到这一点，必须忍受攻击的冲击(虽然可以制定一些安全措施来确保攻击不损害网络)。对此情形，我们不但要采取一些法律手段，而且还要至少请一家有权威的安全公司协助阻止这种犯罪。这类操作的最重要特点就是取得犯罪的证据、并查找犯罪者的地址，提供所拥有的日志。对于所搜集到的证据，应进行有效地保存。在开始时制作两份，一个用于评估证据，另一个用于法律验证。 找到系统漏洞后设法堵住漏洞，并进行自我攻击测试。 网络安全已经不仅仅是技术问题，而是一个社会问题。企业应当提高对网络安全重视，如果一味地只依靠技术工具，那就会越来越被动.只有发挥社会和法律方面打击网络犯罪，才能更加有效。我国对于打击网络犯罪已经有了明确的司法解释，遗憾的是大多数企业只重视技术环节的作用而忽略法律、社会因素，这也是本文的写作目的。 名词解释：拒绝服务攻击(DoS) DoS即Denial Of Service，拒绝服务的缩写，可不能认为是微软的DOS操作系统!DoS攻击即让目标机器停止提供服务或资源访问，通常是

以消耗服务器端资源为目标，通过伪造超过服务器处理能力的请求数据造成服务器响应阻塞，使正常的用户请求得不到应答，以实现攻击目的。