保证Linux系统安全从防范漏洞做起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_ti2020/607/2021_2022__E4_BF_9D_E8_AF_81Linu_c103_607074.htm Linux作为开放式的操作系统受到很多程序员的喜爱，很多高级程序员都喜欢编写Linux操作系统的相关软件。这使得Linux操作系统有着丰富的软件支持，还有无数的技术人员作为技术后盾和技术支持，这使得Linux越来越受到程序员的欢迎。 但这种开放式的操作系统有一个最大的弊端就是每个程序员的水平不等，编写相关软件后并未注意自己程序中的漏洞。没有统一的漏洞检查，这使得 Linux的软件中会出现很多的漏洞，而软件开发者却很难察觉自己编写程序的漏洞，但黑客们会非常注意这些漏洞，并且会利用这些漏洞来达到自己的目的。那么是不是Linux系统就不安全了呢?其实大可不必担心，只要做好下述几点便可安心的使用Linux系统。 一、取消不必要的服务 早期的Unix版本中，每一个不同的网络服务都有一个服务程序在后台运行，后来的版本用统一的/etc/inetd服务器程序担此重任。Inetd是Internetdaemon的缩写，它同时监视多个网络端口，一旦接收到外界传来的连接信息，就执行相应的TCP或UDP网络服务。 由于受inetd的统一指挥，因此Linux中的大部分TCP或UDP服务都是在/etc/inetd.conf文件中设定。所以取消不必要服务的第一步就是检查/etc/inetd.conf文件，在不要的服务前加上“ # ”号。 一般来说，除了http、smtp、telnet和ftp之外，其他服务都应该取消，诸如简单文件传输协议tftp、网络邮件存储及接收所用的imap/ipop传输协议、寻找和搜索资料用的gopher以及用于时间同步的daytime和time等。 还有一

些报告系统状态的服务，如finger、efinger、systat和netstat等，虽然对系统查错和寻找用户非常有用，但也给黑客提供了方便之门。例如，黑客可以利用finger服务查找用户的电话、使用目录以及其他重要信息。因此，很多Linux系统将这些服务全部取消或部分取消，以增强系统的安全性。 Inetd除了利用/etc/inetd.conf设置系统服务项之外，还利用/etc/services文件查找各项服务所使用的端口。因此，用户必须仔细检查该文件中各端口的设定，以免有安全上的漏洞。 在Linux中有两种不同的服务型态：一种是仅在有需要时才执行的服务，如finger服务.另一种是一直在执行的永不停顿的服务。这类服务在系统启动时就开始执行，因此不能靠修改inetd来停止其服务，而只能从修改/etc/rc.d/rc[n].d/文件或用 Runleveleditor去修改它。提供文件服务的NFS服务器和提供NNTP新闻服务的news都属于这类服务，如果没有必要，最好取消这些服务。 二、限制系统的出入 在进入Linux系统之前，所有用户都需要登录，也就是说，用户需要输入用户账号和密码，只有它们通过系统验证之后，用户才能进入系统。 与其他Unix操作系统一样，Linux一般将密码加密之后，存放在/etc/passwd文件中。Linux系统上的所有用户都可以读到 /etc/passwd文件，虽然文件中保存的密码已经经过加密，但仍然不太安全。因为一般的用户可以利用现成的密码破译工具，以穷举法猜测出密码。比较安全的方法是设定影子文件/etc/shadow，只允许有特殊权限的用户阅读该文件。 在Linux系统中，如果要采用影子文件，必须将所有的公用程序重新编译，才能支持影子文件。这种方法比较麻烦，比较简便的方法是采用插入式验证模块(PAM)。很多Linux系统都带有Linux的工具程

序PAM，它是一种身份验证机制，可以用来动态地改变身份验证的方法和要求，而不要求重新编译其他公用程序。这是因为PAM采用封闭包的方式，将所有与身份验证有关的逻辑全部隐藏在模块内，因此它是采用影子档案的最佳帮手。 此外，PAM还有很多安全功能：它可以将传统的DES加密方法改写为其他功能更强的加密方法，以确保用户密码不会轻易地遭人破译.它可以设定每个用户使用电脑资源的上限.它甚至可以设定用户的上机时间和地点。 Linux系统管理人员只需花费几小时去安装和设定PAM，就能大大提高Linux系统的安全性，把很多攻击阻挡在系统之外。 三、保持最新的系统核心 由于Linux流通渠道很多，而且经常有更新的程序和系统补丁出现，因此，为了加强系统安全，一定要经常更新系统内核。 Kernel是Linux操作系统的核心，它常驻内存，用于加载操作系统的其他部分，并实现操作系统的基本功能。由于Kernel控制计算机和网络的各种功能，因此，它的安全性对整个系统安全至关重要。 早期的Kernel版本存在许多众所周知的安全漏洞，而且也不太稳定，只有2.0.x以上的版本才比较稳定和安全，新版本的运行效率也有很大改观。在设定Kernel的功能时，只选择必要的功能，千万不要所有功能照单全收，否则会使Kernel变得很大，既占用系统资源，也给黑客留下可乘之机。 在Internet上常常有最新的安全修补程序，Linux系统管理员应该消息灵通，经常光顾安全新闻组，查阅新的修补程序。 四、增强安全防护工具 SSH是安全套接层的简称，它是可以安全地用来取代rlogin、rsh和rcp等公用程序的一套程序组。SSH采用公开密钥技术对网络上两台主机之间的通信信息加密，并且用其密钥充当身份验证的工具。 由于SSH将网

络上的信息加密，因此它可以用来安全地登录到远程主机上，并且在两台主机之间安全地传送信息。实际上，SSH不仅可以保障Linux主机之间的安全通信，Windows用户也可以通过SSH安全地连接到Linux服务器上。 五、限制超级用户的权力 我们在前面提到，root是Linux保护的重点，由于它权力无限，因此最好不要轻易将超级用户授权出去。但是，有些程序的安装和维护工作必须要求有超级用户的权限，在这种情况下，可以利用其他工具让这类用户有部分超级用户的权限。Sudo就是这样的工具。 Sudo程序允许一般用户经过组态设定后，以用户自己的密码再登录一次，取得超级用户的权限，但只能执行有限的几个指令。 六、设定用户账号的安全等级 除密码之外，用户账号也有安全等级，这是因为在Linux上每个账号可以被赋予不同的权限，因此在建立一个新用户ID时，系统管理员应该根据需要赋予该账号不同的权限，并且归并到不同的用户组中。 在Linux系统上的tcpd中，可以设定允许上机和不允许上机人员的名单。其中，允许上机人员名单在/etc/hosts.allow中设置，不允许上机人员名单在/etc/hosts.deny中设置。设置完成之后，需要重新启动inetd程序才会生效。此外，Linux将自动把允许进入或不允许进入的结果记录到/rar/log/secure文件中，系统管理员可以据此查出可疑的进入记录。 每个账号ID应该有专人负责。在企业中，如果负责某个ID的职员离职，管理员应立即从系统中删除该账号。很多入侵事件都是借用了那些很久不用的账号。 在用户账号之中，黑客最喜欢具有root权限的账号，这种超级用户有权修改或删除各种系统设置，可以在系统中畅行无阻。因此，在给任何账号赋予root权限之前，都必须仔细考虑

。 Linux系统中的/etc/securetty文件包含了一组能够以root账号登录的终端机名称。例如，在RedHatLinux系统中，该文件的初始值仅允许本地虚拟控制台(rtys)以root权限登录，而不允许远程用户以root权限登录。最好不要修改该文件，如果一定要从远程登录为 root权限，最好是先以普通账号登录，然后利用su命令升级为超级用户。 