确保Linux系统安全性的办法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/268/2021_2022__E7_A1_AE_E4_BF_9DLinu_c67_268223.htm 【编者按：Windows由于其使用的普及性，往往成为黑客攻击的对象，但这并不意味着Linux系统就会安全。】 由于Linux操作系统良好的网络功能，因此在因特网中大部分网站服务器都是使用的Linux作为主操作系统的。但由于该操作系统是一个多用户操作系统，黑客们为了在攻击中隐藏自己，往往会选择Linux作为首先攻击的对象。那么，作为一名Linux用户，我们该如何通过合理的方法来防范Linux的安全呢？下面笔者搜集和整理了一些防范Linux安全的几则措施，现在把它们贡献出来，恳请各位网友能不断补充和完善。 1、禁止使用Ping命令 Ping命令是计算机之间进行相互检测线路完好的一个应用程序，计算机间交流数据的传输没有经过任何的加密处理，因此我们在用ping命令来检测某一个服务器时，可能在因特网上存在某个非法分子，通过专门的黑客程序把在网络线路上传输的信息中途窃取，并利用偷盗过来的信息对指定的服务器或者系统进行攻击，为此我们有必要在Linux系统中禁止使用Linux命令。在linux里，如果要想使ping没反应也就是用来忽略icmp包，因此我们可以在Linux的命令行中输入如下命令： echo 1 > /proc/sys/net/ipv4/icmp_echo_igore_all 如果想恢复使用ping命令，就可以输入 echo 0 > /proc/sys/net/ipv4/icmp_echo_igore_all 2、注意对系统及时备份 为了防止系统在使用的过程中发生以外情况而难以正常运行，我们应该对Linux完好的系统进行备份，最好是在一完成Linux系统的安装任务后就对整个系统

进行备份，以后可以根据这个备份来验证系统的完整性，这样就可以发现系统文件是否被非法修改过。如果发生系统文件已经被破坏的情况，也可以使用系统备份来恢复到正常的状态。备份信息时，我们可以把完好的系统信息备份在CD-ROM光盘上，以后可以定期将系统与光盘内容进行比较以验证系统的完整性是否遭到破坏。如果对安全级别的要求特别高，那么可以将光盘设置为可启动的并且将验证工作作为系统启动过程的一部分。这样只要可以通过光盘启动，就说明系统尚未被破坏过。 3、改进登录服务器 将系统的登录服务器移到一个单独的机器中会增加系统的安全级别，使用一个更安全的登录服务器来取代Linux自身的登录工具也可以进一步提高安全。在大的Linux网络中，最好使用一个单独的登录服务器用于syslog服务。它必须是一个能够满足所有系统登录需求并且拥有足够的磁盘空间的服务器系统，在这个系统上应该没有其它的服务运行。更安全的登录服务器会大大削弱入侵者透过登录系统窜改日志文件的能力。 4、取消Root命令历史记录 在linux下，系统会自动记录用户输入过的命令，而root用户发出的命令往往具有敏感的信息，为了保证安全性，一般应该不记录或者少记录root的命令历史记录。为了设置系统不记录每个人执行过的命令，我们可以在linux的命令行下，首先用cd命令进入到/etc命令，然后用编辑命令来打开该目录下面的profile文件，并在其中输入如下内容： HISTFILESIZE=0 HISTSIZE=0 当然，我们也可以直接在命令行中输入如下命令： ln -s /dev/null ~/.bash_history 5、为关键分区建立只读属性 Linux的文件系统可以分成几个主要的分区，每个分区分别进行不同的配置和安装，一般情况下至

少要建立/、/usr/local、/var和/home等分区。/usr可以安装成只读并且可以被认为是不可修改的。如果/usr中有任何文件发生了改变，那么系统将立即发出安全报警。当然这不包括用户自己改变/usr中的内容。/lib、/boot和/sbin的安装和设置也一样。在安装时应该尽量将它们设置为只读，并且对它们的文件、目录和属性进行的任何修改都会导致系统报警。 当然将所有主要的分区都设置为只读是不可能的,有的分区如/var等，其自身的性质就决定了不能将它们设置为只读，但应该不允许它具有执行权限。 6、杀掉攻击者的所有进程 假设我们从系统的日志文件中发现了一个用户从我们未知的主机登录，而且我们确定该用户在这台主机上没有相应的帐号，这表明此时我们正在受到攻击。为了保证系统的安全被进一步破坏，我们应该马上锁住指定的帐号，如果攻击者已经登录到指定的系统，我们应该马上断开主机与网络的物理连接。如有可能，我们还要进一步查看此用户的历史记录，再仔细查看一下其他用户是否也已经被假冒，攻击者是否拥有有限权限；最后应该杀掉此用户的所有进程，并把此主机的IP地址掩码加入到文件hosts.deny中。 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