 世界上没有绝对安全的系统，即使是普遍认为稳定的Linux系统，在管理和安全方面也存在不足之处。我们期望让系统尽量在承担低风险的情况下工作，这就要加强对系统安全的管理。 下面，我具体从两个方面来阐述Linux存在的不足之处，并介绍如何加强Linux系统在安全方面的管理。 防止黑客的入侵 在谈黑客入侵方面的安全管理之前，我先简单介绍一些黑客攻击Linux主机的主要途径和惯用手法，让大家对黑客攻击的途径和手法有所了解。这样才能更好地防患于未然，做好安全防范。 要阻止黑客蓄意的入侵，可以减少内网与外界网络的联系，甚至独立于其它网络系统之外。这种方式虽造成网络使用上的不便，但也是最有效的防范措施。 黑客一般都会寻求下列途径去试探一台Linux或Unix主机，直到它找到容易入侵的目标，然后再开始动手入侵。常见的攻击手法如下： 1、直接窃听取得root密码,或者取得某位特殊User的密码，而该位User可能为root，再获取任意一位User的密码，因为取得一般用户密码通常很容易。 2、黑客们经常用一些常用字来破解密 码。曾经有一位美国黑客表示，只要用“ password ”这个字，就可以打开全美多数的计算机。其它常用的单词还有：account、ald、 alpha、beta、computer、dead、demo、dollar、games、bod、hello、help、intro、kill、 love、no、ok、okay、please、sex、secret、superuser、system、test、work、yes等。 3、使用命令：finger@some.cracked.host，就可以知道该台计算机上面的用

户名称。然后找这些用户下手，并通过这些容易入侵的用户取得系统的密码文件/etc/passwd，再用密码字典文件搭配密码猜测工具猜出root的密码。 4、利用一般用户在/tmp目录放置着的SetUID的文件或者执行着SetUID程序，让root去执行，以产生安全漏洞。 5、利用系统上需要SetUID root权限的程序的安全漏洞，取得root的权限，例如:pppd。 6、从.rhost的主机入侵。因为当用户执行rlogin登录时，rlogin程序会锁定.rhost定义的主机及账号，并且不需要密码登录。 7、修改用户的.login、cshrc、.profile等Shell设置文件，加入一些破坏程序。用户只要登录就会执行，例如“ if /tmp/backdoor exists run /tmp/backdoor ”。 8、只要用户登录系统，就会不知不觉地执行Backdoor程序（可能是Crack程序），它会破坏系统或者提供更进一步的系统信息，以利Hacker渗透系统。 9、如果公司的重要主机可能有网络防火墙的层层防护，Hacker有时先找该子网的任何一台容易入侵的主机下手，再慢慢向重要主机伸出魔掌。例如：使用NIS共同联机，可以利用remote 命令不需要密码即可登录等，这样黑客就很容易得手了。 10、Hacker会通过中间主机联机，再寻找攻击目标，避免被用逆查法抓到其所在的真正IP地址。 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