Linux安全隐患及加强安全管理 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022_Linux_E5_AE_89_E5_85_c103_260897.htm 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。 11、Hacker进入主机有好几种方式，可以经由Telnet（Port 23）、Sendmail（Port25）、FTP（Port 21）或WWW（Port 80）的方式进入。一台主机虽然只有一个地址，但是它可能同时进行多项服务，而这些Port都是黑客“ 进入 ”该主机很好的方式。 12、Hacker通常利用NIS（IP）、NFS这些RPC Service截获信息。只要通过简单的命令（例如showmount），便能让远方的主机自动报告它所提供的服务。当这些信息被截获时，即使装

有tcp_wrapper等安全防护软件，管理员依然会在毫不知情的情况下被“ 借 ”用了NIS Server上的文件系统，而导致/etc/passwd外流。 13、发E-mail给anonymous账号，从FTP站取得/etc/passwd密码文件，或直接下载FTP站/etc目录的passwd文件。 14、网络窃听，使用sniffer程序监视网络Packet，捕捉Telnet，FTP和Rlogin一开始的会话信息，便可顺手截获root密码，所以sniffer是造成今日Internet非法入侵的主要原因之一。 15、利用一些系统安全漏洞入侵主机，例如：Sendmail、Imapd、Pop3d、DNS等程序，经常发现安全漏洞，这对于入侵不勤于修补系统漏洞的主机相当容易得手。 16、被Hacker入侵计算机，系统的Telnet程序可能被掉包，所有用户Telnet session的账号和密码均被记录下，并发E-mail给Hacker，进行更进一步的入侵。 17、Hacker会清除系统记录。一些厉害的Hacker都会把记录它们进入的时间、IP地址消除掉，诸如清除：syslog、lastlog、messages、wtmp、utmp的内容，以及Shell历史文件.history。 18、入侵者经常将如ifconfig、tcpdump这类的检查命令更换，以避免被发觉。 19、系统家贼偷偷复制/etc/passwd，然后利用字典文件去解密码。 20、家贼通过su或sudo之类的Super User程序觊觎root的权限。 21、黑客经常使用Buffer overflow（缓冲区溢位）手动入侵系统。 22、cron是Linux操作系统用来自动执行命令的工具，如定时备份或删除过期文件等等。入侵者常会用cron来留后门，除了可以定时执行破译码来入侵系统外，又可避免被管理员发现的危险。 23、利用IP spoof（IP诈骗）技术入侵Linux主机。 以上是目前常见的黑客攻击Linux主机的伎俩。如果黑客可以利用上述一种方法轻易地入侵计算机的话，

那么该计算机的安全性实在太差了，需要赶快下载新版的软件来升级或是用patch文件来修补安全漏洞。在此警告，擅自使用他人计算机系统或窃取他人资料的都是违法行为，希望各位读者不要以身试法。 除了上面这些方法，很多黑客还可以利用入侵工具来攻击Linux系统。这些工具常常被入侵者完成入侵以后种植在受害者服务器当中。这些入侵工具各自有不同的特点，有的只是简单地用来捕捉用户名和密码，有的则非常强大可记录所有的网络数据流。总之，黑客利用入侵工具也是攻击Linux主机的常用方法。 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