如何提高 Linux 系统的安全性

Linux 系统不论在功能上、价格上或性能上都有很多优点，然而，作为开放式操作系统，它不可避免地存在一些安全隐患。关于如何解决这些隐患，为应用提供一个安全的操作平台，本文会告诉你一些最基本、最常用，同时也是最有效的招数。

Linux 是一种类 Unix 的操作系统。从理论上讲，Unix 本身的设计并没有什么重大的安全缺陷。多年来，绝大多数在 Unix 操作系统上发现的安 全问题主要存在于个别程序中，所以大部分 Unix 厂商都声称有能力解决这些问题，提供安全的 Unix 操作系统。但 Linux 有些不同，因为它不属于某一家 厂商，没有厂商宣称对它提供安全保证，因此用户只有自己解决安全问题。

Linux 是一个开放式系统，可以在网络上找到许多现成的程序和工具，这既方便了用户，也方便了黑客，因为他们也能很容易地找到程序和工具来潜入 Linux 系统 ,或者盗取 Linux 系统上的重要信息。不过 ,只要我们仔细地设定 Linux 的各种系统功能，并且加上必要的安全措施，就能让黑客们无机可乘。

一般来说 ,对 Linux 系统的安全设定包括取消不必要的服务、限制远程存取、隐藏重要资料、修补安全漏洞、采用安全工具以及经常性的安全检查等。本文教你十种提高 Linux 系统安全性的招数。虽然招数不大 ,但招招奏效 ,你不妨一试。

1、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 Run level editor 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。

2、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。

3、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。

4、检查登录密码

设定登录密码是一项非常重要的安全措施，如果用户的密码设定不合适，就很容易被破译，尤其是拥有超级用户使用权限的用户，如果没有良好的密码，将给系统造成很大的安全漏洞。

在多用户系统中，如果强迫每个用户选择不易猜出的密码，将大大提高系统的安全性。但如果 passwd 程序无法强迫每个上机用户使用恰当的密码，要确保密码的安全度，就只能依靠密码破解程序了。

实际上，密码破解程序是黑客工具箱中的一种工具，它将常用的密码或者是英文字典中所有可能用来作密码的字都用程序加密成密码字，然后将其与 Linux 系统的/etc/passwd 密码文件或/etc/shadow 影子文件相比较，如果发现有吻合的密码，就可以求得明码了。

在网络上可以找到很多密码破解程序，比较有名的程序是 crack.用户可以自己先执行密码破解程序，找出容易被黑客破解的密码，先行改正总比被黑客破解要有利。

5、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。

6、消除黑客犯罪的温床

在 Unix 系统中 ,有一系列 r 字头的公用程序 ,它们是黑客用以入侵的武器，非常危险，因此绝对不要将 root 账号开放给这些公用程序。由于这些公用程序都是用。rhosts 文件或者 hosts.equiv 文件核准进入的，因此一定要确保 root 账号不包括在这些文件之内。

由于 r 字头指令是黑客们的温床 ,因此很多安全工具都是针对这一安全漏洞而设计的。例如，PAM 工具就可以用来将 r 字头公用程序的功力废掉，它在 /etc/pam.d/rlogin 文件中加上登录必须先核准的指令，使整个系统的用户都不能使用自己 home 目录下的。rhosts 文件。

7、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。

8、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。例如，应用 sudo 后，可以让管理磁带备份的管理人员每天按时登录到系统中 ,取得超级用户权限去执行文档备份工作，但却没有特权去作其他只有超级用户才能作的工作。Sudo 不但限制了用户的权限，而且还将每，希望以上的提高 Linux 系统安全性的招数对大家有用。