# 基于Linux系统的网络安全问题及其对策

**作者：浙江财经学院东方学院　张琳俊**

一、 linux系统用户信息基本安全机制

1、 口令安全

口令安全可以说是系统的第一道防线,目前网上的大部分对系统的攻击都是从截获口令或猜测口令开始的，所以我们应该选择更加安全的口令， 杜绝不设口令的账号存在。
我们可以通过查看/etc/passwd 文件，例如，存在用户 skylinq 的账号，如下：skylinq::501:501::/home/skylinq:/bin/bash；其中第二项为空，说明skylinq这个用户账号没有设置密码。

2、影子文件(/etc/shadow)的安全

在系统中任何一个合法用户都可以查看/etc/passwd这个文件，因此给用户口令的安全性带来了较大的隐患,所以在linux系统中通过/etc/shadow文件把口令加密信息隐藏起来。该文件默认只有超级用户 root 才能读，一旦/etc/shadow 文件信息被窃取，就可以通过穷举法获得用户账号密码。所以/etc/shadow文件的安全性直接影响用户口令的安全。

3、 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。

4、 加密技术

加密时要用到密匙，密匙是一个特殊的数字，把密匙和需要加密的信息经过加密算法加密之后，只有知道密匙的人才能把信息读出来。如果所有的计算机主机都在你的控制下，加密当然是一个好方法，但是，如果其中一台“被信任的”主机被黑客控制了，你马上就有危险了。这就不仅仅是用户的帐号和口令有危险了。在通常情况下，加密是用来保证机密信息在系统中传送的安全。如果一台计算机被控制了，那么这些加密信息就会让人知道或是泄密了。有一个好的安全策略，这种危险的可能性会降到最低，但是如果某台主机的密匙被泄露出去，那么危险始终存在。

5 、linux文件系统权限设置

Linux文件系统的安全主要是通过设置文件的权限来实现的。每一个Linux的文件或目录，都有3组属性，分别定义文件或目录的所有者，用户组和其他人的使用权限（只读、可写、可执行、允许SUID、允许SGID等）。特别注意，权限为SUID和SGID的可执行文件，在程序运行过程中，会给进程赋予所有者的权限，如果被黑客发现并利用就会给系统造成危害。

二、网络安全基础

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。

2、合理划分子网和设置防火墙

如果内部网络要进入 Internet，必须在内部网络与外部网络的接口处设置防火墙，以确保内部网络中的数据安全。对于内部网络本身，为了便于管理，合理分配 IP 地址资源，应该将内部网络划分为多个子网，这样做也可以阻止或延缓黑客对整个内部网络的入侵。

3、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。

4、保持最新的系统核心

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。因为内核的安全性对整个系统安全至关重要。

三、网络安全防范

在此，我们不对各类进攻者进行区分，我们将其统称为黑客。为了准确地对黑客攻击实施防范策略，首先对黑客进攻的类型、原理、方法和步骤等进行分析，然后我们可以制定相应的防范措施。

1、黑客进攻行为分析

黑客进攻行为通常有以下四种类型：(1)信息窃取和盗用(2)信息欺诈和勒索(3)信息攻击和破坏(4)信息污染和滥用。

(1）黑客入侵步骤

黑客为什么要入侵某一目标？除非本身就是怀有特定的目的外，一般是偶然的因数居多，但在偶然的因素下面必然有许多必然的原因，如系统本身存在的安全漏洞等因素，让黑客有机可趁。黑客往往采用一下几个步骤实现入侵目标主机的目的。[2]

(2）寻找目标主机并分析目标主机

在 internet 网上真正标示主机的是 ip 地址，只要利用域名和 ip 地址就可以顺利地找到目标主机。此时，黑客们常会使用一些扫描工具，轻松获得目标系统运行的版本，系统有哪些账户，WWW，FTP，Telnet,SMTP 等服务器程序是哪种版本，为入侵做准备。

(3）获取账号和密码，登入主机

黑客要想入侵一台主机，首先要有主机的一个账号和密码，否则连登入都无法进行。这

样常迫使黑客先设法盗窃账户文件，进行破译，从中获取某用户的账号和口令，再寻觅时机以此身份进入主机。当然，利用某些工具或系统漏洞登入主机也是黑客的一种技法。

(4）获得超级用户权限，控制主机

黑客有了普通账号，便可以利用 FTP、Telnet 等工具进入目标主机。在进入目标主机后，黑客一般不会就此罢手的，因为普通用户的权限实在有限，所以他们会设法获得超级用户权限。

(5）“拒绝服务”攻击

所谓“拒绝服务”攻击是指黑客采取具有破坏性的方法阻塞目标网络的资源，使网络暂时或永久瘫痪，从而使 Linux 网络服务器无法为正常的用户提供服务。例如黑客可以利用伪造的源地址或受控的其他地方的多台计算机同时向目标计算机发出大量、连续的 TCP/IP 请求，从而使目标服务器系统瘫痪。

(6）“扫描程序和网络监听”攻击

许多网络入侵是从扫描开始的，利用扫描工具黑客能找出目标主机上各种各样的漏洞，并利用之对系统实施攻击。

网络监听也是黑客们常用的一种方法，当成功地登录到一台网络上的主机，并取得了这台主机的超级用户控制权之后，黑客可以利用网络监听收集敏感数据或者认证信息，以便日后夺取网络中其他主机的控制权。

2、黑客防范措施

(1）合理利用 Linux 的日志文件

Linux 的日志文件用来记录整个操作系统使用状况。作为一个 Linux 系统管理员要充分用好以下几个日志文件。

①/var/log/secure 文件

记录登入系统存取数据的文件，例如 pop3，ssh，telnet，ftp 等都会记录在此文件中。

②/var/log/wtmp 文件

记录当前和历史上登录到系统的用户的登录时间、地点和注销时间等信息。可以用 last 命令查看，若想清除系统登录信息，只需删除这个文件，系统会生成新的登录信息。

③/var/log/messages 文件

这个文件相当重要，几乎系统发生的所有错误信息（或重要信息）都会记录在这个文件中。

(2）制定适当的数据备份计划确保系统万无一失

没有一种操作系统的运转是百分之百可靠安全的，也没有一种安全策略是万无一失的，因此作为 Linux 系统管理员，必须为系统制定适当的数据备份计划，充分利用磁带机、光盘刻录机、双机热备份等技术手段为系统保存数据备份，使系统一旦遭到破坏或黑客攻击而发生瘫痪时，能迅速恢复工作，把损失减少到最少。

时至今日，对于危及系统和网络安全的多数保护手段还相对较弱，而随着 Linux 的流行且高速 Internet 存取逐渐实现的时刻，涌向未经预防的 Linux 系统的攻击会越来越多。作为 Linux 系统的管理员，头脑中一定要有安全防范意识，定期对系统进行安全检查，发现漏洞要立即采取措施，不给黑客以任何可乘之机。

参考文献:

[1]鸟 哥.鸟哥的 linux 私房菜. 科学出版社.
[2]肖德琴.电子商务安全保密技术与应用.华南理工大学出版社.
[3]潘 瑜.基于 Linux 系统的网络安全策略.计算机基础教程网.
[4]梁如军.丛日权,Red Hat Linux9 网络服务.机械工业出版社.