第10章　服务器的安全性概述

Internet上任何一台计算机都是网络黑客试图攻击的对象，安全问题显得尤为重要。特别是对于企业和教育单位的网络服务器而言，地址和服务项目的公开使得黑客的攻击有了目标和可能利用的漏洞，例如，对于未作防范的计算机，只需要简单地通过 telnet就可以知道正在使用的Linux版本号，就像这样：

```
Red Hat Linux release 5.2 (Appolo)
Kernel 2.0.36 on an i686
Login:
```

黑客可以利用版本的漏洞有针对性地发起攻击。特别是有些低版本的 Linux，其安全性漏洞已经广为流传，黑客可以很容易地侵入。而网络服务器往往储存了大量的重要信息，或向大量用户提供重要服务；一旦遭到破坏，后果不堪设想。所以，网站建设者更需要认真对待有关安全方面的问题，以保证服务器的安全。

10.1　服务器安全管理

10.1.1　安全防护的主要内容

对于网站管理人员而言，日常性的服务器安全保护主要包括四方面内容：

文件存取合法性：任何黑客的入侵行为的手段和目的都可以认为是非法存取文件，这些文件包括重要数据信息、主页页面 HTML文件等。这是计算机安全最重要的问题，一般说来，未被授权使用的用户进入系统，都是为了获取正当途径无法取得的资料或者进行破坏活动。良好的口令管理(由系统管理员和用户双方配合)，登录活动记录和报告，用户和网络活动的周期检查都是防止未授权存取的关键。

用户密码和用户文件安全性：这也是计算机安全的一个重要问题，具体操作上就是防止已授权或未授权的用户相互存取相互的重要信息。文件系统查帐、 su登录和报告、用户意识、加密都是防止泄密的关键。

防止用户拒绝系统的管理：这一方面的安全应由操作系统来完成。操作系统应该有能力应付任何试图或可能对它产生破坏的用户操作，比较典型的例子是一个系统不应被一个有意使用过多资源的用户损害(例如导致系统崩溃)。

防止丢失系统的完整性：这一方面与一个好系统管理员的实际工作 (例如定期地备份文件系统，系统崩溃后运行fsck检查、修复文件系统，当有新用户时，检测该用户是否可能使系统崩溃的软件)和保持一个可靠的操作系统有关 (即用户不能经常性地使系统崩溃)。

10.1.2　Linux系统的文件安全

Linux的文件系统是由文件和目录构成的树形结构，每个文件目录记录包括下面内容(域)：

- 文件名
- 文件类型
- 文件大小
- 文件创建修改时间
- 文件所有者和所有组
- 文件相关权限

任何一项内容遭受未授权的修改，文件安全性都遭到破坏。保护文件系统的安全性，应该从以下几个方面入手。

1. 文件相关权限的设置

Linux的文件权限决定了用户对该文件的操作能力和操作允许范围。下面这一段是在某个Linux用户目录的文件列表(ls -l)，注意，其中第一栏表示了文件权限。

```
drwxrwxr-x  3   bluo  bluo  1024     Apr 7   17:07 php/
drwxr-xr-x  16  bluo  bluo  4096     Apr 8   12:46 php-3.0.12/
-rw-rw-r--  1   bluo  bluo  1857165  Apr 8   12:37 php-3.0.12.tar.gz
drwxr-xr-x  12  bluo  bluo  4096     Apr 8   11:51 php-4.0b1/
-rw-rw-r--  1   bluo  bluo  1304415  Apr 7   12:11 php-4.0b1.tar.gz
-rw-r--r--  1   bluo  bluo  2023424  Dec 28  21:10 php.pdf
-rw-r--r--  1   bluo  bluo  44409    Mar 16  22:34 pre_video.jpg
drwxr-xr-x  3   bluo  bluo  1024     Apr 10  11:30 public_html/
```

文件权限通过设置文件权限标志位实现。标志位由十位构成。第一位是文件类型，一般文件该位为“ - ”，目录该位为“ d ”(如上面的1、2、4、8行)。余下的九位三位一组，第二位到第四位依次为文件所有者对此文件的可读、可写、可执行权利标志位；第五到第七位分别为与该用户同组的用户对此文件的可读、可写、可执行的权利标志位：第八到第十位分别为其他用户对此文件的可读、可写、可执行的权利标志位。比如：上面的第一个目录中，“ drwxrwxr-x ”就表示这是一个目录，文件所有者 (用户bluo)可以对文件进行任何操作 (读、写、执行)，同组用户可读、写、执行，其他用户可读和执行。而“ -rw-r--r-- ”表示普通文件，文件所有者可读、写，其他用户只可读此文件。当一些关键的系统文件的属性被错误设置时，就会导致不可挽回的破坏。对文件属性一定要非常小心，否则可能导致致命的安全漏洞。

2. SUID和SGID程序

与文件有关的还有两个附加权限位 SUID和SGID。SUID是SetUserID(设置用户标识)的缩写，SGID是SetGroupID(设置组标识)的缩写。带有这种权限的程序运行时就会带来很大的安全性漏洞。因为当运行一个 SUID程序时，它的有效UID被设置为拥有该程序的用户 ID，而不管实际上是哪个用户在运行，SGID与此类似。所以虽然SUID程序是必需的，但应该尽量减少使用机会，并且要尽最大努力保证此程序安全。作为管理员还应该经常使用 find命令来浏览自己的文件系统以检查新的SUID程序，详细语法请参考文件权限章节中的相关内容。

10.1.3 用户访问安全

1. 口令安全

每个Linux的用户都拥有一个帐号，通过登录到这个帐号才能有限制地使用系统。而保护自身的文件安全的惟一屏障就是口令，一旦这道屏障被突破，此用户及整个系统的安全便无

法得到保证。

从安全角度看，口令最好是随机产生的，并且不断变换的。但实际上任何一个用户都不愿意成天花费时间去记忆刚刚更换过的口令，这是一对矛盾。所以用户应该做到尽可能保持频繁的口令更换频率，并且聪明地选择自己的口令保证其安全。切忌选用与自己有关的一些数字、名词、住址、配偶名称、宠物名称、电话号码等，更不要选用字典中的词汇作为口令。因为当今使用的很多破解口令程序都是通过一定的加密算法将字典中的词汇一个一个与口令作比较，以期闯入系统。另外从概率角度讲，口令位数每增加一位，被破解的可能性就会相差很多数量级，因此在系统允许的范围内尽可能长地设置自己的口令实为明智之举。

那么怎么选择一个好口令呢？这里推荐三种常用方法：一是选择一个自己比较熟悉的短语或者是谚语，取出每个单词或者某短句中每个汉字对应的拼音的第一或者某一位组合起来形成口令，这样一来形成的口令接近于随机字符序列，但同时也容易记忆。比如：好好学习天天向上。得到的口令就是：hhxxttxs。二是选择两个较短的单词，其间用符号或者某特定的字母加以连接，比如：dear-user-linux。还有一种方法是采用一个故意拼写错误的单词，比如：Limux；或者使用故意加入语法错误的短语，比如： a-girls。这样产生的口令被破解的机会就小多了。

最后最关键的是用户应当牢牢记住自己的口令，最好不要把口令写在任何地方，只有自己的脑袋是保险的。如果实在是对记忆能力缺乏信心，那么也建议将口令藏在某个不起眼的短句中。比如：口令是box！Here，那么将Don’t touch the top of box！Here！写到一张纸条上，贴在电源上就显得非常自然。

2. 登录安全

如果用户口令得到了良好的保证，那么紧接着的第二部分就是登录和帐号的安全性问题。这便涉及在系统中查找可能有安全问题的帐号并及时处理。

首先很多黑客是使用没有口令的帐号进入计算机系统的，作为管理员应该经常检查口令文件，查找这种帐号，一旦发现，应该立刻通知用户或者禁止其使用。

其次对于不使用的帐号应该及时删除，使之不至于成为黑客进入的通道。即使不删除此帐号，至少也应该在口令字段写入符号，暂时停止此帐号的使用。

再次，对于几个标准系统帐号，一般情况下应该禁止这些帐号的使用。因为这些帐号几乎是每个非法闯入者的目标，即使使用再好的口令，也有被破解的可能，所以最安全的办法就是禁止其使用。还有一些软件在安装过程中会自动在系统中创建帐号，所以一定要注意禁止这些帐号的使用。

对于匿名访问者帐号 (guest)，一般情况下是不建议使用的。这种帐号是为来访者提供的帐号，使他们能够使用本机上的某些资源，获得部分权限。但同时由于 guest帐号一般不设密码，所以也是进入系统的捷径。黑客进入系统以后可以进一步获得更高的权限，可能导致安全性灾难。黑客将尽力取得root权限，同时以此为基点进攻网络上其他的机器，这使得追查其来源更加不容易。所以尽可能不要使用 guest帐号。

系统中还有几个命令帐号，也就是运行给定命令然后退出。这些帐号没有口令，虽然它们并不运行shell，但是从安全方面也是极其危险的。比如使用 finger登录时，finger程序便运行起来，显示该系统用户，显示后结束运行。类似的帐号还有 sync和date。这种帐号可能会泄

露系统的有关信息。系统安全实际上是由登录帐号和对应口令共同保证的，如果入侵者获得了系统用户的帐号，那他已经成功了一半。

最后是关于组帐号的问题。组帐号是供多人使用的同一个帐号。这对系统安全是极为不利的。因为如果组帐号被人闯入，那么寻找泄露口令的用户是非常困难的。所以建议创建帐号时遵循“一个帐号一个用户”的原则。

10.1.4 日常安全注意事项

1) 删除系统所有默认的帐号和密码，这些帐号往往是黑客攻击时的第一目标，特别注意保护root用户密码。

2) 在用户合法性得到验证前不要显示公司题头、在线帮助以及其他信息，使黑客试图侵入前获得的信息尽可能少。

3) 废除“黑客”可以攻击系统的所有不在使用的网络服务，如匿名 ftp等，每一项网络服务程序都包括这样那样的漏洞，启用的服务越多，系统安全漏洞也就越多。

4) 使用6到8位的字母数字混合的密码，并经常更换密码。可以设置用户密码的安全等级和有效期限，注意，安全等级过高的系统，用户密码的设置会非常麻烦。

5) 限制用户尝试登录到系统的次数，防止黑客通过“穷举法”破译密码。在密码输入错误次数达到某限制值时，帐号将被锁定。

6) 记录违反安全性的情况并对安全记录进行复查。

7) 对于重要信息，上网传输前要先进行加密。现在已经有了很多的加密传输协议，并且有了相关标准，可以根据需要选用。

8) 重视专家提出的建议，安装他们推荐的系统“补丁”。各种版本的Linux都在不断地推出各种“补丁”程序，它们有的修正系统 BUG，有的提供功能扩展，还有的修改系统安全漏洞，这就是安全管理所需要的内容。

9) 限制不需密码即可访问的主机文件。

10) 修改网络配置文件，以便将来自外部的 TCP连接限制到最少数量的端口。不允许诸如tftp、sunrpc、printer、rlogin或rexec之类的协议。

11) 用upas代替sendmail。sendmail有太多已知漏洞，很难修补完全。

12) 去掉对操作并非至关重要又极少使用的程序。

13) 使用chmod将所有系统目录变更为 711模式。这样，攻击者们将无法看到它们当中有什么东西，而用户仍可执行。

14) 只要可能，就将磁盘安装为只读模式。其实，仅有少数目录需读写状态。

15) 将系统软件升级为最新版本。老版本可能已被研究并被成功攻击，其安全漏洞早已广为流传，最新版本一般包括了这些问题的补丁，高版本总是更加稳定可靠的。

10.1.5 服务器被侵入后的处理

虽然采取了很多安全措施，但是还是有可能被侵入。一旦服务器遭到网络黑客的攻击，应该及时采取下述行动：

首先设法使服务器进入安全状态，即将入侵者清理出系统，如果实在没有办法，就断开所有网络连接(拔掉网线或者关闭调制解调器)。

不要急于恢复系统，那样可能覆盖掉黑客入侵的行动记录和留下的蛛丝马迹，而这些东西是将来反黑客的重要线索。一定要设法寻找出入侵者是如何进入的，然后弥补好这个漏洞以免被再次侵入。如果不能弥补，宁愿关闭掉该项服务，否则即有可能继续遭到攻击。另外要特别注意用户文件和口令，防止黑客为下次攻击留下“后门”。

然后要通过系统备份来恢复被损坏或者删除的文件，这是必须要做的，系统恢复以后就可以重新网络开始服务了。

最后，如果入侵继续发生，则求救于本地的其他管理员，寻求技术支持。有时甚至需要通过法律手段来保护网站安全。

10.2 防火墙、IP伪装和代理服务器

10.2.1 什么是防火墙

防火墙是汽车中一个部件的名称。在汽车中，利用防火墙把乘客和引擎隔开，汽车引擎一旦着火，防火墙不但能保护乘客安全，同时还能让司机继续控制引擎。在电脑中，防火墙是一种装置，可使个别网络不受公共部分 (整个Internet)的影响。

本文将防火墙电脑称为“防火墙”，它能同时连接受到保护的局域网络和 Internet两端。这样受到保护的网络无法连接到 Internet，Internet也无法连接到受到保护的网络。如果要从受到保护的网络内部接到 Internet网络，就得telnet到防火墙，然后从防火墙连上 Internet。最简单的防火墙是dual homed系统(具有两个网络联结的系统)。只要配置一台Linux主机(配置时将IP forwarding/gateweying 设为OFF)，并为每人设一帐户，他们就能登录这一主机，使用 telnet、FTP，阅读电子邮件和使用所有这台主机提供的任何其他服务。根据这项配置，这一网络中惟一能与外界联系的电脑便是这个防火墙。

Linux 2.2.x内核用ipchains代替了原来2.0内核中的ipfwadm。ipchains较之以前的ipfwadm语法变动很大，如果想了解更多的命令和语法，可以参考 ipchains howto (http://www.hncd.gov.cn/linux)，或者运行ipchains -help。

10.2.2 防火墙分类

1. IP过滤防火墙

IP过滤防火墙在IP层工作。它依据起点、终点、串口号和每一数据包中所含的数据包种类信息控制数据包的流动。这种防火墙非常安全，但是缺少有用的登录记录。它阻挡别人进入个别网络，但不能记录何人进入公共系统，或何人从内部进入网际网。过滤防火墙是绝对性的过滤系统。即使要让外界的一些人进入私有服务器，用户也无法让每一个人进入服务器。Linux从1.3.x版开始就在内核中包含了数据包过滤软件。

2. 代理服务器

代理服务器允许通过防火墙间接进入网际网。最好的例子是 telnet到系统，然后从该处再telnet到另一个系统。在有代理服务器的系统中，这项工作就完全自动完成。利用客户端软件连接代理服务器后，代理服务器启动它的客户端软件 (代理)，然后传回数据。由于代理服务器重复所有通信，因此能够记录所有进行的工作。只要配置正确，代理服务器就绝对安全，这是它最可取之处。由于没有直接的IP通路，它阻挡任何人进入。

10.2.3 Linux防火墙实现策略

一般而言，实现Linux防火墙功能有两种策略：

一种是首先全面禁止所有的输入/输出/转发包，然后根据需要逐步打开所要求的各项服务，这种方式最安全，但必须全面考虑到自己所要使用的各项服务功能，不能有任何遗漏。如果用户对要实现的某种服务和功能不能清楚地知道应该打开哪些服务和端口，就会比较麻烦。

第二种方式是首先默认打开所有的输入/输出包，然后禁止某些危险包、IP欺骗包、广播包、ICMP服务类型攻击等，对于应用层服务像http、sendmail、pop3、ftp等，若不打算提供某些服务，就不要启动它，或者根本就不要安装。这种方式虽然没有第一种方式更安全，但是比较方便，容易配置，用户不必过多地了解该如何打开一种服务所需要执行的ipchains命令细节就能配置一个比较安全的防火墙系统。