第 10 章　网络操作系统安全

本章分为两大部分，第一部分主要阐述 Windows 的系统加固安全问题，第二部分阐述 Linux 系统的安全设置问题。第一部分主要介绍加固 Windows 系统安全的几种方法，如安装更新包、关闭不必要的服务、账号安全管理等；在 Linux 系统的安全设置部分中主要介绍用户账户的管理、服务进程的设置、文件的访问权限、日志系统的设置以及常用的安全工具。

- 安装最新的系统补丁 Service Pack 与更新 HotFix 程序
- 关闭不必要服务和账号安全管理
- 激活 Windows 审核功能
- 文件权限管理
- Linux 网络和系统服务
- Linux 后台服务进程
- Linux 文件的访问权限
- Linux 的日志系统的设置

10.1　Windows 系统的安全加固

10.1.1　安装最新的系统补丁 Service Pack 与更新 HotFix 程序

微软公司为提高其开发的各种版本的 Windows 操作系统的市场占有率，会及时地将软件产品中发现的重大问题以安全公告的形式公布于众，这些公告都有一个唯一的编号，即 MS-，如 MS03-063，MS 是微软的英文缩写，03 代表 2003 年，063 代表该安全公告的编号，合起来就是微软公司在 2003 年发布的第 63 个安全公告。每个公告都有一个补丁程序，就是 HotFix，当 HotFix 累计到一定程度，微软就会以 SP（Service Pack）的方式把此前的 HotFix 整合起来。为了保证网络操作系统的安全，我们必须随时关注微软的这些补丁程序，下面就针对 HotFix 和 Service Pack 展开讨论。

1. 更新 HotFix 程序

更新 HotFix 程序之前我们可以先考查一下自己使用的操作系统里已经有了哪些补丁程序，进而确定是否更新 HotFix 程序。其方法如下：

打开“控制面板”中的“添加与删除程序”，然后在最右上方单击“显示更新”。便可以在

下面的控制台窗口中看到本机上的 Hotfix，如图 10-1 所示就是 Windows XP 的软件更新情况。

图 10-1　Windows XP 的 HotFix 安装情况

如果系统内没有安装最新的 HotFix，有多种方法可用来执行更新安装 HotFix，包括搭配安装选项来手动执行 HotFix.exe 程序、使用 Systems Management Server（SMS），以及使用 Windows Installer 等。

2. 安装最新的系统补丁 Service Pack

Service Pack 可使产品保持最新。Service Pack 包括更新、系统管理工具、驱动程序和其他组件，它们捆绑在一起以便下载。前文介绍过 Service Pack 具有累积性。因此，每个新的 Service Pack 中不仅包含新的修复程序，还包含以前 Service Pack 中包括所有修复程序。在安装最新的 Service Pack 之前，视不同版本来确定是否需要安装以前的 Service Pack。例如，在安装 Windows 2003 Service Pack 2（SP2）之前不需要先安装 Windows 2003 Service Pack 1（SP1）。

10.1.2　管理员账户的安全管理

用户账户是计算机安全设置的重要对象，许多安全功能的实现都是基于用户账户的，如文件访问权限设置、用户环境设置等。系统管理员账户可以完全控制其他普通用户账户，包括创建、禁用、删除等；所以管理员账户的安全管理是保障系统安全的重要条件。

默认情况下，管理员账户是 Windows 系统中权限最高的账户，拥有管理员权限，也就相当于拥有了整个系统或网络。因此，管理员账户就成为黑客们的主要攻击目标。作为网络和计算机管理员，尤其应该做好管理员账户的安全管理，如更改账户名称、设置密码、创建陷阱账户等，避免被破解或盗取。

1. 更改 Administrator 账户名

按照默认设置安装完 Windows Server 2003 或 Windows Server 2008 后，都会创建一个系统管理员账户，即 Administrator。许多用户贪图一时方便，就直接使用系统管理员账户，因此，许多黑客攻击服务器时，总是试图破解 Administrator 账户的密码，如果此时密码安全性不高，则后果不堪设想。通常情况下，可以通过更改管理员账户名称来避免此类攻击，提高系统安全性。

（1）更改本地计算机 Administrator 账户名。以 Administrator 账户登录本地计算机，依次选择“开始”→“管理工具”→“本地计算机管理”选项，打开“地计算机管理”窗口，展开“系统工具”→“本地用户和组”→“用户”，右击 Administrator 账户并选择“重命名”选项，稍后输入新的账户名称即可，如图 10-2 所示。设置新的账户名称时，尽量不要使用 Admin、master、guanliyuan 之类的名称，否则账户安全性同样没有任何保障。

图 10-2 “计算机管理”窗口

（2）更改域 Administrator 账户名。默认情况下，域中的所有用户账户存放在域控制器的 Users 容器中，Administrator 账户是整个域的超级管理员用户。依次选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，显示如图 10-3 所示的“Active Directory 用户和计算机”窗口，在 Users 容器中右击 Administrator 账户，选择快捷菜单中的“重命名”选项。

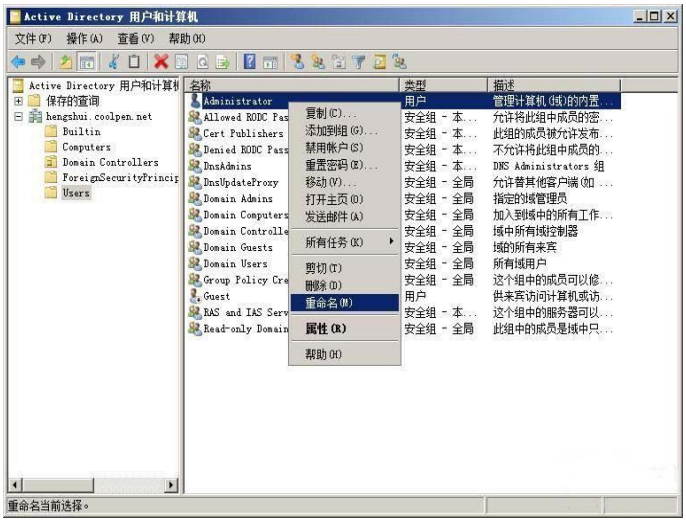

图 10-3 “Active Directory 用户和计算机”窗口

（3）通过组策略更改 Administrator 账户名。无论是独立计算机还是域控制器，都可以通过 Windows 组策略更改 Administrator 账户名称。如果是独立计算机，则可以依次选择“开始”

→“管理工具”→“本地安全策略”选项，打开“本地安全策略”控制台；依次展开“安全设置”→“本地策略”→“安全选项”选项，在右侧主窗口中双击“账户：重命名系统管理员账户”，打开“账户：重命名系统管理员账户”对话框，如图 10-4 所示，重新输入新的账户名称即可。

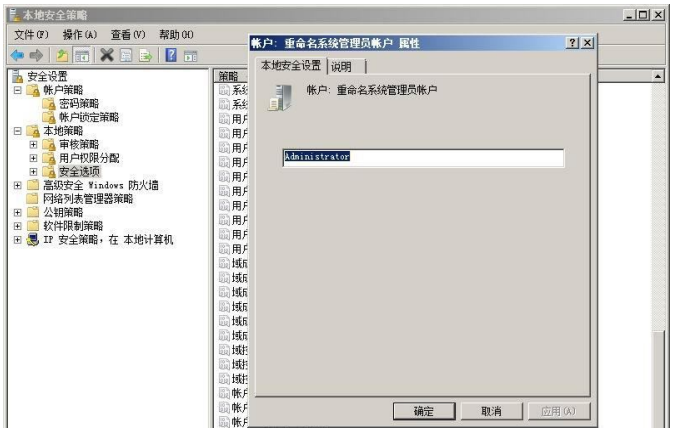

图 10-4　通过本地安全策略更改管理员账户名

如果是域控制器，则需要依次选择“开始”→“管理工具”→“组策略管理”选项，找到作用于根域的默认策略“Default Domain Policy”，右击并选择快捷菜单中的“编辑”选项，打开“组策略管理编辑器”窗口，依次展开“策略”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，双击右侧主窗口中的“账户：重命名系统管理员账户”，打开“账户：重命名系统管理员账户属性”对话框，系统默认没有定义该策略，选中“定义这个策略设置”复选框，并在文本框中输入新的名称即可，如图 10-5 所示。

图 10-5　通过域安全策略更改管理员账户名

2. 禁用 Administrator 账户

在 Windows Server 2003 和 Windows Server 2008 操作系统中，Administrator 账户是超级管理员，拥有整个系统乃至网络的所有权限。如果更改账户名仍然无法达到安全需求，可以选择直接将其禁用，然后创建一个普通的管理员账户，用于实现基本的系统或者网络管理、

维护功能。

在“计算机管理”控制台的“本地用户账户和组”→“用户”窗口中，双击 Administrator 打开如图 10-6 所示的“Administrator 属性”对话框，选中“账户已禁用”复选框即可。如果是 Windows 域控制器，则可以在“Active Directory 用户和计算机”的“Users”容器中，进行此设置。

禁用 Administrator 账户与为其更名相比，安全性更高。但是，当需要完成某些特殊管理任务而要用到超级管理员账户时，必须先进入安全模式，重新启用该账户，如进行目录恢复和还原等。

用户自定义的管理员，虽然同样属于某些系统管理员组，但却无法获得超级管理员的终极权限，功能方面仍有很大区别。

3. 减少管理员组成员

尽量减少管理员组成员的数量，也是最大限度保证网络安全的重要措施。由于管理员组成员拥有对系统的各种操作、配置和访问权限。因此，从某种意义上来讲，限制了管理员组的成员数量，也就限制了拥有较高权限的用户和密码管理的难度，减少容易被识破的密码被用于系统密码的机会，从而避免使系统处于危险的境地。

对于独立计算机而言，可以在“计算机管理”→“本地用户和组”→“组”中，双击 Administrators 打开如图 10-7 所示的“Administrators 属性”对话框，选择“成员”列表中想要删除的管理员账户，并单击“删除”按钮即可。如果是域控制器，则除了减少 Administrators 组中的成员之外，还应严格控制添加到 DnsAdmins 组和 Enterprise Admins 组中的成员账户，这些组同样是 Administrators 组中的成员。

图 10-6 “Administrator 属性”对话框（一）

图 10-7 “Administrators 属性”对话框（二）

系统管理员的数量越少，密码丢失或被猜到的可能性就越小，相对而言，系统也就越安全。因此，除非必要，不要将技术水平不高的用户添加为管理员组成员。

4. 系统管理员口令设置

入侵者若想盗取系统内的重要数据信息或执行某项管理功能，就必须先获得管理员权限，即破解管理员账户密码。弱密码会使得攻击者易于破解而得以访问计算机和网络，而强密码则难以破解，即使是密码破解软件也难以办到。

密码破解软件的工作机制主要包括三种：巧妙猜测、词典攻击和自动尝试字符组合。从理论上讲，只要有足够时间，使用这些方法可以破解任何账户密码，破解一个弱密码可能只需要几秒钟即可完成，而要破解一个安全性较高的强密码则可能需要几个月甚至几年的时间。因此，系统管理员账户必须使用强密码，并且经常更改密码。

（1）注意事项。在设置管理员账户密码时，应注意以下问题：

1）切不可让账号与密码相同。如果将用户账号与密码设置为相同，许多系统扫描工具默认将账户和密码作为相同的设置扫描系统，无疑会省去攻击者的很多力气。

2）切不可使用自己的姓名。对于本单位和熟悉本单位的人而言，姓名无疑是攻击的首选，因为这几乎谁都能猜得到。另外，在许多黑客编写的字典中，往往将百家姓一一列出，并放在字典的前列。

3）切不可使用英文词组。一些常用或别致的英文单词往往是用户设置密码时的最爱，这类密码既便于记忆，又凸显自己的个性。但事实上，黑客也早已猜到并详细地将其编入字典，因此，英文词组也是绝不可用的。

4）切不可使用特定意义的日期。以具有特定意义的日期作为密码是任何人都十分喜爱的，这一类日期通常有自己生日、父母生日、儿女生日、朋友生日、重大节日、个人纪念日等。不用说熟悉的人可以猜得到，即使是陌生人也可以通过穷举的方式而得手。在黑客字典中，几乎全部罗列以上所有的几个组合，实在令人惊骇不已。

5）切不可使用简单的密码。字符数越少、密码越简单，在破解时所用的时间就越短。一个穷举软件每秒钟可以重试 10 万次之多，字数越少，字符越简单化，排列组合的结果也就越少，也就越容易被攻破。

（2）安全密码原则。若要保证账户密码的安全，应当遵循以下规则：

用户密码应包含英文字母的大小写、数字、可打印字符，甚至是非打印字符，将这些符号排列组合使用，以期达到最好的保密效果。

用户密码不要太规则，不要将用户姓名、生日和电话号码作为密码。不要用常用的单词作为密码。

根据黑客软件的工作原理，参照密码破译的难易程度，以破解需要的时间为排序指标，密码长度设置时应遵循 7 位或 14 位的整数倍原则。

在通过网络验证密码过程中，不得以明文方式传输，以免被监听截取。

密码不得以明文方式存放在系统中，确保密码以加密的形式写在硬盘上，且包含密码的文件是只读的。加密的方法很多，如基于单向函数的密码加密，基于测试模式的密码加密，基于公钥加密方案的密码加密，基于平方剩余的密码加密，基于多项式共享的密码加密，基于数字签名方案的密码加密等。经过上述方法加密的密码，即使是系统管理员也难以得到。

密码应定期修改，以避免重复使用旧密码，应采用多套密码的命名规则。

建立账号锁定机制。一旦同一账号密码校验错误若干次即断开连接并锁定该账号，经过一段时间才解锁。

由网络管理员设置一次性密码机制，用户在下次登录时必须更换新的密码。

10.1.3　关闭不必要的服务

提高系统安全性涉及到许多方面，其中重要的一步是关闭不必要的服务。下面以 Windows

XP 为例阐述关闭不必要的服务的方法。

1. 关闭 IIS 服务

IIS 微软的互联网信息服务（IIS）提供了将用户的计算机变成一个 Web 服务器的能力。这项服务可以通过以下方法关闭：打开“控制面板”，找到“添加或删除程序”，单击“添加/删除 Windows 组件”，取消选择“Internet 信息服务（IIS）”即可。

2. 关闭 NetMeeting 远程桌面共享服务

NetMeeting 远程桌面共享：网络会议主要是一个 Windows 平台的 VoIP 和视频会议客户端，不过这种服务仅对远程桌面访问才需要。

3. 关闭远程桌面帮助会话管理器服务

远程桌面帮助会话管理器（Remote Desktop Help Session Manager）：这种服务可以允许其他人远程访问你的系统，帮助你解决问题。

4. 关闭远程注册表服务

远程注册表：这种能力从安全的观点来看是相当可怕的。因为它允许远程用户能够编辑 Windows 的注册表。

5. 关闭路由器和远程访问服务

路由器和远程访问服务：这种服务包含了多种能力，这些能力正是多数系统管理员可能会需要单独提供的。这些服务中的任何一个对于一个典型的桌面系统，如对 XP 来说都是必要的，然而，作为一项单独的服务它们又需要关闭。路由选择和远程访问提供了一种将系统用作路由器和 NAT 设备的能力，或者作为一个拨号访问网关，或者作为一个 VPN 服务器。如果你不想让设备发挥这种功能，完全可以将其禁用。

6. 关闭简单文件共享服务

简单文件共享（Simple File Sharing）服务：如果一台计算机并不是微软 Windows 域的一部分，默认情况下所有的文件共享是可以从任何地方访问的。然而，在现实世界中，我们只想将共享提供给特定的、授权的用户。同样地，简单文件共享只是无一例外地允许共享提供给所有用户，这并不是共享文件系统的初衷。默认情况下，在 Windows XP 的专业版和家用版中，这种功能是活动的。不过，它无法在家用版中禁用。在专业版中，可通过这种方法将其关闭：打开“我的电脑”→“工具”菜单”→“文件夹选项”→“查看”选项卡，取消选择“高级设置”下的“使用简单文件共享（推荐）”，如图 10-8 所示。

7. 关闭 SSDP 发现服务

SSDP 发现服务：也称为简单发现服务，这种服务用于发现网络上的 UpnP 设备，“通用即插即用设备主机 Universal Plug and Play Device Host”需要这项服务，如图 10-9 所示。

8. 关闭 Telnet（远程登录）服务

Telnet（远程登录）服务：远程登录服务是一项很老的机制，可以提供对一台计算机的远程访问。现在，很少使用 Telnet 远程管理一个系统，取而代之的是一种加密协议即 SSH。因此完全可以禁用远程登录。

9. 关闭 Universal Plug and Play Device Host 服务

Universal Plug and Play Device Host 服务：即前面所说的“通用即插即用设备主机”服务，虽然许多用户在系统中安装了这项服务，其实并不太实用。

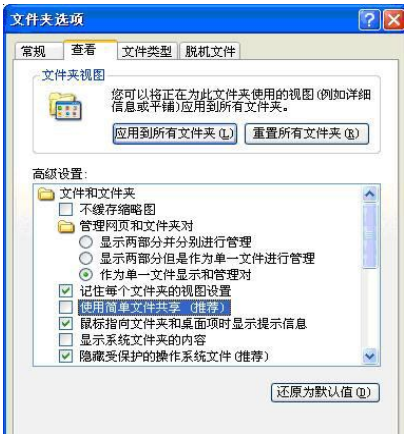

图 10-8　“文件夹选项”对话框

图 10-9　“系统配置实用程序”对话框

在你的系统上，这些服务可能并没有全部打开或安装。一个特定的服务是否安装或运行依赖于安装系统时的选择，不管你是否在运行 XP 家用版或专业版。

除了上述的简单文件共享，其他所有的服务都可以采用相同的方式禁用。最简单的方法即：依次打开“控制面板”→“管理工具”→“服务”，如图 10-10 所示。

要想禁用列表中的某项服务，可以在其上双击，在弹出的窗口中选择“启动类型”单击“停止”即可完全关闭某种服务。一般说来，用户为了安全的需要应将某项服务设为“禁用”的状态。其方法是：在某项服务上右击选择属性，在弹出的窗口中选择“启动类型”后下拉列表中的“已禁用”，然后单击“确定”按钮即可。

可以这样说，每一项正在运行但却未用的服务就是计算机上的一个安全漏洞。如果某项服务对授权用户和基本的系统功能来说并不重要，就需要关闭它。

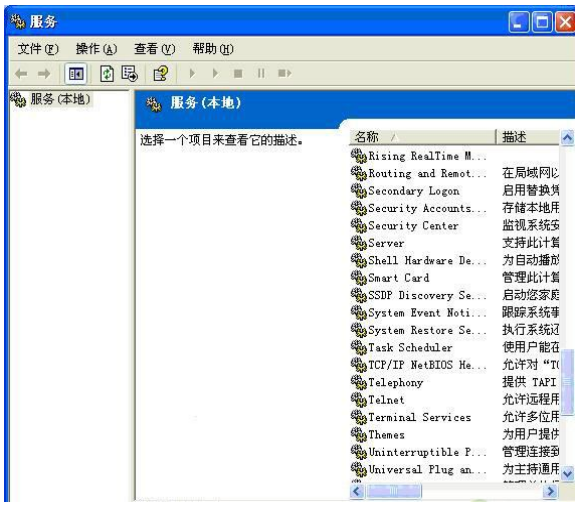

图 10-10　“Windows 服务”窗口

10.1.4　激活系统的审核功能

审核是用来跟踪用户的活动及网络中发生的各种事件。通过审核，可以将一项指定的行

为或事件记录在安全日志中。一条审核记录应该解决的问题和包含的内容：审计的对象（审计谁）、发生的行为（审什么）、实施该行为的用户（谁审计）、行为发生的时间和日期（何时审）、何时清除审计结果，以及制定合适的审计方案等。

安全审核系统也是网络操作系统中安全系统的非常重要的组成部分，它是对身份验证系统和资源访问控制系统的必要补充。安全审核系统可以保证在网络安全出现问题时，记录当前信息，为排除安全故障提供至关重要的信息。Windows 提供了三个事务审核与跟踪的系统，即安全日志、系统日志和应用程序日志。

1. 审核策略的拟定与实施

在拟定和实现一份审核策略时，应考虑和注意如下一些因素。

（1）明确所审核的类型和事件。常见的审计类型有 3 类：系统审计、应用程序审计和用户自行配置的安全性审计等。例如：用户的登录及登录退出、文件或目录的使用、关闭和重新启动 Windows NT Server、用户和组的改变以及安全规则的改变等。

（2）明确审核的是事件的成功，还是失败的记录。

1）跟踪事件的成功记录能了解文件和打印机的访问频率，从而有助于进行资源规划。

2）跟踪事件的失败记录，将对非法入侵发出警报。

3）在中等和高等安全的网络中，应该跟踪用户登录成功和失败的记录，及资源的使用情况。

2. 安全审核系统的设置

在 Windows 系统网络中审核系统的设置可以分成两个主要部分：其一，设置选定计算机中需要审核的事件；其二，设置其他要审核对象的审核事件如文件、目录和打印机等对象的审核事件等。

在 PDC 上可以设置域的审计事件。设置 PDC 计算机中需要审核事件的步骤如下：

（1）选择“开始”→“程序”→“管理工具（公用）”→“域用户管理器”激活“域用户管理器”窗口。

（2）选择“规则”→“审核（D）”选项，激活如图 10-11 所示的“审核规则”对话框。

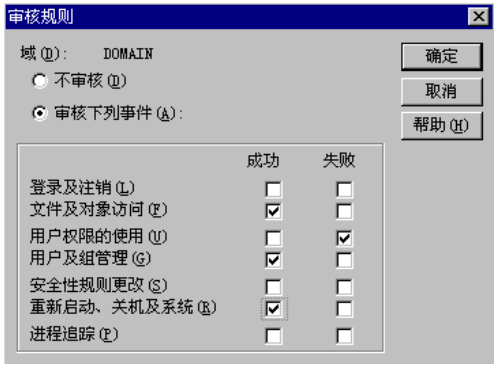

图 10-11 “域用户管理器”中的“审核规则”对话框

（3）在图 10-11 所示的对话框中，管理员既可以审核成功的操作，也可审核失败的操作。当选择某安全事件之后，可以将复选框打上“√”。

（4）系统可以审核的事件说明如下：

1）登录及注销：指用户的登录或登录退出。通过网络与一台服务器建立连接或断开连接。

2）文件及对象访问：指设置了用户访问目录、文件和打印机的审核。

3）用户权限的使用：指用户使用了某种权力（有关登录或登录退出的权力除外）。

4）用户及组管理：指创建、删除或重新使用一个用户账户或组，更改用户口令，重新命名、禁止或重新使用一个用户账户。

5）安全性规则（策略）更改：指更改用户权力，审核规则或信任关系。

6）重新启动、关机及系统：指用户重新启动或关闭计算机，或者是影响到系统安全或安全日志的事件，例如：安全日志已经满了。

7）进程追踪：指对各种事件的详细跟踪记录信息，例如程序的启动。

完成上述的设置之后，应当进一步的设置其他要审核对象的审核事件。例如：可选择或指定的其他可审核的对象有文件、目录和打印机等。

3. 使用事件查看器查看审计的数据

安全审核系统将审核的结果保存在系统的各种日志中，管理员通过事件查看器可以查看系统的日志。事件查看器可以提供出错信息、警告信息，以及执行某项任务的成功或者失败等内容的具体信息。这些信息存放在以下 3 类日志内：

（1）系统日志：包括系统产生出错信息、警告信息以及提示信息。这是由 Windows NT 预先设定好的。

（2）安全日志：包括设置审核事件成功或是失败的信息。这些事件都是在审核规则中设定的。

（3）应用日志：包括应用程序产生的出错信息，警告信息以及提示信息。这是由程序开发者事先设定好的。

10.1.5　文件权限管理

网络中最主要的资源就是文件和目录，因此，几乎所有操作系统的访问控制机制的安全特性都取决于文件和目录的安全性。当然，文件和目录的安全也是 Windows 安全模型的核心。文件和目录的安全性可以应用于单个文件、多个文件、目录或整个的目录结构。因此，Windows 的资源访问控制系统，可以确定用户对目录和文件的访问和使用的权利。它除了规定了用户所能访问的网络信息资源的目录和文件外，还可以控制用户的访问层次和范围。

一、通过共享许可（权限）保护网络资源

1. 共享的基本概念

共享和共享文件夹：当一个目录（文件夹）被共享时，用户就可以通过网络连接到该共享目录（文件夹）上，进而访问该文件夹中的所有文件和文件夹。因此，共享是一种开放共享资源的操作，而所开放的目录资源就被称为共享目录。

2. 共享许可（权限）

（1）共享许可。在共享许可情况下，用户可以通过共享目录（文件夹）来访问网络的程序、数据和用户的宿主文件夹，但不能对目录下的文件具有单独和特定的权限。此外，当用户从本地登录访问资源时，共享目录设置的权限（许可）是无效的。

（2）共享许可使用的目的。其基本目的是：避免网络中的每个用户都安装同样的文件和目录。共享许可应用的另一个目的：是将安全性运用于网络的共享资源上，例如：共享许可运用于目录上，可以实现共享目录的网络安全访问。

（3）FAT 分区中的共享许可。在 FAT 分区上，共享许可是使网络资源获得安全性的唯一方法。

（4）共享目录许可（权限）的类型。共享目录许可的类型有 4 种，由高到低依次表示为：完全控制、更改、读取与拒绝访问。

3. 用户和组的共享许可

如果管理员需要控制用户对共享目录的访问，就要给用户分配共享目录的访问权限。共享资源的权限既可以被单独地分配给用户或组；也可以被同时分配给组和用户。因此，一个用户既可以直接获得某个目录的使用权限，也可以作为组的成员获得该目录的使用权限。一般情况下，用户对某个资源的有效权限为用户权限和组权限的组合，即取用户和组权限中的较高权限。例如：如果用户对于某个目录具有了“读取”权限，同时 Everyone 组被分配了该目录“完全控制”的访问权限。则由于该用户必定是 Everyone 的组员，因此，用户和组的组合权限的结果是该用户对于这个目录具有“完全控制”的访问权限。

4. 对于用户和组分配共享许可的一般准则

- 对被访问的资源确定允许访问的组。
- 给组分配其应具有的访问许可的类型。
- 在允许网络用户执行所需的任务的前提下，给共享资源分配最严格的权限。
- 删除新共享文件夹上的给 Everyone 组分配的“完全控制”的缺省权限。

5. 共享目录的权限（许可）的应用

下面从网络安全的角度出发，将介绍为共享目录分配许可（权限）的步骤。

（1）依次选择“开始”→“程序”→“资源管理器”命令，打开资源管理器窗口。

（2）选择要管理的“驱动器”→“目录”，右击，在激活的快捷菜单中选择“属性”选项。

（3）在所选目录的“属性”对话框选择“共享”选项卡，在该对话框中即可对以下内容进行设置。

“共享名”选项处应输入该目录的共享名。应注意：管理员或用户可以通过在共享名后，加一个“$”符号来创建一个隐藏的共享目录，当用户在浏览计算机时，“$”符号可以将此共享目录隐藏起来。拥有该隐藏目录使用许可的用户仍然可以使用它。

“用户个数”选项：输入使用该资源的确定用户数目。

“备注”选项：用于输入该共享资源的描述，通过描述能够标识共享目录的内容，该选项处可以空白。

（4）在“属性”对话框中，单击“权限”按钮。在激活的对话框中，可以为用户或组分配选定目录的使用权限。此处，应先选择用户和组，再为其分配权限类型。可以选择的访问类型有“完全控制”、“读取”和“拒绝访问”等。

对于一个已共享的目录，管理员可以执行“停止该目录的共享”的操作。当然，管理员必须注意，如果停止一个用户正在使用的目录，则可能导致用户数据的丢失。因此，当需要停止目录的共享时，会出现一个对话框提醒有用户正连接到该共享目录上。

二、通过 NTFS 许可保护网络资源

Windows 操作系统中可以利用 NTFS 文件系统，而不是 FAT 文件系统来格式化硬盘的。在 NTFS 分区中可以通过共享许可和文件的目录许可两种方式实现网络资源的安全保护。由此可见，在 NTFS 分区上，除了能够实现文件和目录的共享之外，还能够在文件和目录一级实施

安全措施。

1. NTFS 许可（权限）

（1）NTFS 许可：NTFS 许可（权限）就是只能在 NTFS 文件系统分区上使用的权限。

（2）使用 NTFS 权限（许可）的目的：共享许可只能控制网络资源的访问，而不能阻止从本地登录时对硬盘的任何操作；即使用共享许可的用户可以通过本地的交互式登录，从本地访问文件和目录，因此，共享许可不能保护目录和单个的文件。而 NTFS 许可（权限）不但能够控制远程登录用户的访问，还能限制本地登录用户操纵文件和目录的能力。此外，在 NTFS 中，还可以审核任何个人和组访问文件和目录事件的成败情况，即用户的权限可以分配给目录和单独的文件，所以采用 NTFS 可以提供更高的安全性。

（3）NTFS 许可类型：可以按文件和目录许可分为两大类，即文件许可和目录许可两类。每类 NTFS 许可又可以分别包括 NTFS 的标准许可和 NTFS 的特殊访问许可两类。

NTFS 的标准许可（权限）：包括标准文件许可和标准目录许可两类。在大多数情况下，Windows NT 的文件系统中都使用 NTFS 标准许可

NTFS 的特殊访问许可（权限）：包括特殊文件访问许可和特殊目录访问许可两类。

1）文件许可：用于控制对文件的访问。文件许可又可以进一步分为标准文件许可和特殊访问文件许可两类。

- 标准文件许可的类型：拒绝访问（None）、读取（RX）、更改（RWXD）和完全控制（All）4 种。
- 特殊访问文件许可的类型：读取（R）、写入（W）、执行（X）、删除（D）、更改许可权（P）和获得所有权（O）6 种。

2）目录许可：用于控制对 NTFS 分区中各目录的访问。目录许可也可以进一步分为标准目录许可和特殊访问目录许可两类。

- 标准目录许可的类型（文件和目录的访问权利）：拒绝访问（None 和 None）、列表（RX 和未指定）、读取（RX 和 RX）、添加（WX 和未指定）、添加与读取（RWX 和 RX）、更改（RWXD 和 RWXD）和完全控制（All）7 种。
- 特殊访问目录许可的类型：完全控制（All）、读取（R）、写入（W）、执行（X）、删除（D）、更改许可权（P）和获得所有权（O）等 7 种。

注意：

- 在 NTFS 分区上创建目录或文件的用户将成为该文件或目录的所有者，而所有者总是能够分配和改变资源权限的。
- NTFS 中文件的权限高于该文件存放目录所分配的权限。例如：一个用户对一个目录拥有“写入”权限，对这个目录中的某个文件却只有“读取”的权限时，则用户对该文件的权限是“读取”。

对于组账户和用户账户设置、使用和管理 NTFS 权限的方法与 FAT 文件系统中共享权限（许可）的类似，一个用户既可以被直接分配权限，也可作为组的成员被分配权限。

在共享许可中，权限可以分配给用户和组，但共享许可只能提供有限的安全性。

在 NTFS 许可中，通过 NTFS 许可和共享许可的组合，而获得网络资源的最大程度的安全性，在这两个许可中，限制最严格的权限是用户最终得到的有效权限。

2. 分配 NTFS 许可（权限）的准则

- 移去给 Everyone 组的完全控制许可。
- 给管理员组（Administrator 组）分配完全控制许可。
- 对数据文件夹的创建组（Creator Owner 组）分配完全控制许可。
- 让用户为自己的文件分配 NTFS 许可。
- 在完成任务的前提下，为用户分配最严格的权限。

3. 应用和分配 NTFS 许可时的操作步骤

（1）在 NTFS 系统分区上的 NT-SER 或 NT-WS 上，依次选择“开始”→“程序”→“资源管理器”命令，打开“资源管理器”窗口。

（2）选择要管理的目录或文件后，右击，在激活的快捷菜单中选择“属性”选项。

（3）在激活的选定目录或文件的“属性”对话框中选择“安全性”选项卡，从中选择并单击“权限”按钮。

（4）在激活的对话框中，通过选择“访问类型”来为当前的组和用户分配权限。在该对话框中，所见到的是 NTFS 的标准权限。另外，从“访问类型”列表中，可以通过选择“选择性目录访问”和“选择性文件访问”选项，进一步扩充目录的访问权限。

（5）选定之后，单击“添加”按钮，在激活的对话框中，可以为其他的用户和组分配所目录或文件的 NTFS 权限。最后单击“确定”按钮，完成对组或用户 NTFS 目录权限的分配任务。

10.2 Linux 系统安全加固

对于开放式的操作系统 Linux，系统的安全设定包括系统服务最小化、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。

10.2.1 最新安全补丁

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的安全至关重要。

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。

10.2.2 用户账号

在 Linux 系统中，用户账号是用户的身份标志，它由用户名和用户口令组成。系统将输入

的用户名存放在/etc/passwd 文件中，而将输入的口令以加密的形式存放在/etc/shadow 文件中。在正常情况下，这些口令和其他信息由操作系统保护，能够对其进行访问的只能是超级用户（root）和操作系统的一些应用程序。但是如果配置不当或在一些系统运行出错的情况下，这些信息可以被普通用户得到。进而不怀好意的用户就可以使用一类被称为“口令破解”的工具去得到加密前的口令。

（1）删除系统特殊的用户账号和组账号。

（2）用户密码设置。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。

（3）修改自动注销账号时间。自动注销账号的登录，在 Linux 系统中 root 账户是具有最高特权的。如果系统管理员在离开系统之前忘记注销 root 账户，那将会带来很大的安全隐患，应该让系统可以自动注销。通过修改账户中 TMOUT 参数，可以实现此功能。

（4）给系统的用户名密码存放文件加锁。

（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，并且分配到不同的用户组中。

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。

（6）限制超级用户的权力。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。

10.2.3　网络和系统服务

一、限制网络访问

1. NFS 访问

如果使用 NFS 网络文件系统服务，应该确保/etc/exports 具有最严格的访问权限设置，也

就是意味着不要使用任何通配符、不允许 root 写权限并且只能安装为只读文件系统。编辑文件/etc/exports 并加入如下两行：

/dir/to/export host1.myd o main.com（ro，root_squash）

/dir/to/export host2.myd o main.com（ro，root_squash）

/dir/to/export 是想输出的目录，host.myd o main.com 是登录这个目录的机器名，ro 意味着 mount 成只读系统，root_squash 禁止 root 写入该目录。为了使改动生效，运行如下命令：

/usr/sbin/exportfs -a

2. Inetd 设置

首先要确认/etc/inetd.conf 的所有者是 root，且文件权限设置为 600。设置完成后，可以使用“stat”命令进行检查。

chmod 600 /etc/inetd.conf

然后，编辑/etc/inetd.conf 禁止以下服务。

ftp telnet shell login exec talk ntalk imap pop-2 pop-3 finger auth

如果安装了 ssh/scp，也可以禁止掉 Telnet/FTP。为了使改变生效，运行如下命令：

#killall -HUP inetd

默认情况下，多数 Linux 系统允许所有的请求，而用 TCP_WRAPPERS 增强系统安全性是举手之劳，可以修改/etc/hosts.deny 和/etc/hosts.allow 来增加访问限制。例如，将/etc/hosts.deny 设为"ALL: ALL"可以默认拒绝所有访问。然后在/etc/hosts.allow 文件中添加允许的访问。例如，"sshd: 192.168.1.10/255.255.255.0 gate.openarch.com"表示允许 IP 地址 192.168.1.10 和主机名 gate.openarch.com 允许通过 SSH 连接。

配置完成后，可以用 tcpdchk 检查：

tcpdchk

tcpchk 是 TCP_Wrapper 配置检查工具，它检查你的 tcp wrapper 配置并报告所有发现的潜在/存在的问题。

3. 登录终端设置

/etc/securetty 文件指定了允许 root 登录的 tty 设备，由/bin/login 程序读取，其格式是一个被允许的名字列表，可以编辑/etc/securetty 且注释掉如下的行。

tty1 # tty2 # tty3 # tty4 # tty5 # tty6

这时，root 仅可在 tty1 终端登录。

4. 避免显示系统和版本信息

如果希望远程登录用户看不到系统和版本信息，可以通过以下操作改变/etc/inetd.conf 文件：

telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd -h

加-h 表示 telnet 不显示系统信息，而仅仅显示"login:"。

二、系统服务

在 Linux 系统的服务管理方面，如果做到服务的最全面的安全，其中主要的就是升级服务本身的软件版本，另外一个就是关闭系统不使用的服务，做到服务最小化。

1. 关闭系统不使用的服务

cd /etc/init.d ##进入到系统 init 进程启动目录

在这里有两个方法，可以关闭 init 目录下的服务：①将 init 目录下的文件名 mv 成*.old 类

的文件名，即修改文件名，作用就是在系统启动的时候找不到这个服务的启动文件；②使用 chkconfig 系统命令来关闭系统启动等级的服务。

2. 给系统服务端口列表文件加锁

主要作用：防止未经许可的删除或添加服务

chattr +i /etc/services

3. 修改 ssh 服务的 root 登录权限

修改 ssh 服务配置文件，使 ssh 服务不允许直接使用 root 用户来登录，这样减少系统被恶意登录攻击的机会。

10.2.4　后台服务进程

服务进程（Daemon）是 Linux 操作系统的核心程序，是外界与主机互相交互的主要途径，同时也是连接 Internet 的大门。

1. 配置独立的专用服务器，增加负荷能力，降低风险

Linux 作为优秀的网络操作平台，完全有能力胜任运行多个服务器。比如，它可以作为 Web 服务器，同时也可以充当 FTP 服务器和 Mail 服务器。这样做的好处在于能够降低投资成本，但是不安全因素也会随之相应增加。因此，需要在投资成本与安全最大化之间权衡。假如电脑连接 Internet，提供多种服务，且每天都要提供大量访问量时，建议一：“不要把所有的鸡蛋放在同一个篮子里”。把各个服务进程运行在不同的主机上，成为专用的 Web 服务器，FTP 服务器或 Mail 服务器，共同分担风险。建议二：把各种服务分类管理。在 FTP 服务器和 Mail 服务器访问量不大时，也可以把它们统一管理。

2. 取消所有非必要的服务，尽量做到干净，减少后门

把 Linux 作为专用服务器是个明智的举措。例如，希望 Linux 成为强大的 Web 服务器，可以取消系统内所有非必要的服务，只开启必要服务。这样做可以尽量减少后门，降低隐患，而且可以合理分配系统资源，提高整机性能。以下是几个不常用的服务：

（1）fingerd（finger 服务器）报告指定用户的个人信息，包括用户名、真实姓名、shell、目录和联系方式，它将使系统暴露在不受欢迎的情报收集活动下，应避免启动此服务。

（2）R 服务（rshd、rlogin、rwhod、rexec）提供各种级别的命令，它们可以在远程主机上运行或与远程主机交互，在封闭的网络环境中登录而不再要求输入用户名和口令，相当方便。然而在公共服务器上就会暴露问题，导致安全威胁。

（3）X-Window 从严格的意义上说，是 Linux 窗口管理器的扩展，而不是重要的组成部分。从目前的 GNOME、KDE 这两种主流图形服务器来看，体积越来越臃肿，耗存越来越大，一些基于图形界面的软件在使用上也存在不少问题。虽然开发人员不会放弃对它的完善，但对于服务器来说，它的存在价值几乎没有。因此，在安装服务器时，务必考虑是否真的需要图形管理界面。

（4）其他服务，如 amd、arpwatch、atd、dhcpd、innd、nntpd、talkd、lpd、named、routed、snmpd、xfs、wuftpd、tftpd、telnet、ypbind、yppasswd、ypserv，既然是 Web 服务器，都可以取消或卸载掉。

同理，如果是作为 FTP 服务器运行，只需 FTP 进程和必要的程序。

3. 安全系数高的服务替代正在运行的服务进程

对于一些必要的服务器，如之前所说的 Web 服务器，理论上只需要 Apache 的进程就可以工作了。但是如果管理员需要远程控制放在运营中心的主机呢？或者用户需要通过 FTP 上传更新资料呢？而 Telnet、wu-ftp 这些服务的安全性太低，这时，就需要启用安全级别高的服务来替代这些服务程序。以下为几个需要替代的进程：

（1）用 OpenSSH 替代 Telnet。推荐使用开放软件 OpenSSH（Secure Shell），这是一个安全的登录系统，且不受加密方法的出口限制，适用于替代 Telnet、rlogin、rsh、rcp、rdist。另外，OpenSSH 也可以用来在两台计算机间建立一条加密信道供其他不安全软件使用。OpenSSH 支持多种算法，包括 BlowFish、Triple DES、IDEA、RSA。目前支持 SSH 的客户端软件不少，推荐使用 Putty 和 Filezilla。关于服务器和软件的安装使用，请参见相关文章，在此不再详述。

（2）用 Vsftpd 替代 wu-ftpd、tftpd（基本的 FTP 服务）、ncftpd（匿名服务）。如果想要一个优秀的 FTP 软件，建议使用 Vsftpd。Vsftpd（Very Secure）是一个非常值得信赖的 FTP 软件。除了与生俱来的高安全性外，在 ASCII 传输模式下的速度是 wu-ftpd 的两倍，在千兆以太网的下载速度可达 86Mb/s；在稳定性方面，Vsftpd 可以在单机（非集群）上支持 4000～15000 个以上的并发用户同时连接。除此以外，还可以建立虚拟 FTP 服务器，支持非系统用户的登录下载，同时也可以给不同的用户分配不同的权限，保证服务的安全最大化。现在世界上很多著名的公司都在使用 Vsftpd，如 Red Hat、GNU、GNOME、SuSe、KDE、OpenBSD 等。具体安装和配置请见参考资料。

（3）用 Qmail 替代 Sendmail。Sendmail 将来仍然是主要的 SMTP 服务器，网络上有关 Sendmail 服务器的配置资料随处可见。但事实上由于 Sendmail 代码的复杂性，使得很多人对其配置一知半解。多数情况下，新手们往往只要能够让 Sendmail 启动起来、能收发邮件就觉得万事大吉了。这样的配置其实漏洞太多，难以保证安全性。所以，Qmail 是个更好的选择。当然，要想真正建立一个功能强大、运行稳定的邮件服务器，掌握其灵活的配置，认真阅读 How-to 手册和 FAQ 是很有必要的。

4. 使用 tcpwrappers 控制文件

在没有设置防火墙之前，可以通过一种简单而可靠的机制——tcpwrappers 来加强网络访问控制。tcpwrappers 从两个文件中读取网络访问控制规则：

/etc/hosts.allow 指定授权主机

/etc/hosts.deny 指定非授权主机

配置文件的编写规则非常简单，一般是：

services_list : client_list [: shell_command]

其中 services_list 可以列出一个或几个服务进程名，也可以使用通配符；client_list 可以是 IP 地址、主机名或者网络号，也可以使用通配符。

services_list 有两个特殊用法的符号：ALL 和 EXCEPT。ALL 表示所有的进程，而 EXCEPT 表示排除某个进程。比如，ALL EXCEPT in.fingerd 表示除了 in.fingerd 以外所有的进程。

10.2.5 文件/目录访问许可权限

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。

SUID 和 SGID 攻击方式的预防：

（1）严格审查系统内的文件权限。可以找出系统内使用 SUID/SGID 的文件，列出清单保存，做到心中有数。命令如下：

[root#] find / -type f -perm +6000 -ls | less

[root#] find / -type f -perm +6000 > Suid-Sgid.txt

（2）对于一部分程序必须设置为 SUID 的，可以让它们自成一组，集中管理。但是绝对不允许在用户的家目录下有 SUID 程序存在。

（3）确保重要的 SUID 脚本不可写。命令如下：

[root#] find / -perm -2 ! -type l -ls

（4）对于并非绝对需要被设置成 SUID 的程序，改变它们的访问权限或者卸载程序。如：

[root#] chmod -s [program]

（5）查找系统内所有不属于任何用户和组的文件。因为这些文件很容易被利用来获得入侵主机的权限，造成潜在的威胁。命令如下：

[root#] find / -nouser -o -nogroup

（6）善于使用 lsattr 和 chattr 这两个 ext2/3 的属性命令。

如果主机直接暴露在 Internet 或者位于其他危险（如其他非管理员亦可接触服务器）环境，有很多 Shell 账户或提供 HTTP 和 FTP 等网络服务，一般应该在安装配置完成后使用如下命令，便于保护这些重要目录：

[root#] chattr -R +i /bin /boot /etc /lib /sbin

[root#] chattr -R +i /usr/bin /usr/include /usr/lib /usr/sbin

[root#] chattr +a /var/log/messages /var/log/secure.....

如果很少对账户进行添加、变更或删除操作，把/home 本身设置为 Immutable 属性也不会造成什么问题。

在很多情况下，整个/usr 目录树也应该具有不可改变属性。实际上，除了对/usr 目录使用 chattr -R +i /usr/命令外，还可以在/etc/fstab 文件中使用 ro 选项，使/usr 目录所在的分区以只读的方式加载。

10.2.6　日志系统

1. 系统引导日志

使用 dmesg 命令可以快速查看最后一次系统引导的引导日志。通常它的内容会很多，所以往往会将其通过管道传输到一个阅读器。

2. 系统运行日志

（1）Linux 日志存储在/var/log 目录中。这里有几个由系统维护的日志文件，但其他服务和程序也可能会把它们的日志放在这里。大多数日志只有 root 才可以读，不过只需要修改文件的访问权限就可以让其他人可读。

以下是常用的系统日志文件名称及其描述：

- lastlog：记录用户最后一次成功登录时间。
- loginlog：不良的登录尝试记录。
- messages：记录输出到系统主控台以及由 syslog 系统服务程序产生的消息。
- utmp：记录当前登录的每个用户。
- utmpx：扩展的 utmp。
- wtmp：记录每一次用户登录和注销的历史信息 wtmpx 扩展的 wtmp。
- vold.log：记录使用外部介质出现的错误。
- xferkig：记录 Ftp 的存取情况 sulog 记录 su 命令的使用情况。
- acct：记录每个用户使用过的命令。
- aculog：拨出自动呼叫记录。

（2）/var/log/messages。messages 日志是核心系统文件。它包含了系统启动时的引导消息，以及系统运行时的其他状态消息。IO 错误、网络错误和其他系统错误都会记录到这个文件中。其他信息，比如某个人的身份切换为 root，也在这里列出。如果服务正在运行，比如 DHCP 服务器，你可以在 messages 文件中观察它的活动。通常，/var/log/messages 是你在做故障诊断时首先要查看的文件。

（3）/var/log/XFree86.0.log。这个日志记录的是 Xfree86 XWindows 服务器最后一次执行的结果。如果你在启动到图形模式时遇到了问题，一般情况从这个文件中会找到失败的原因。

（4）在/var/log 目录下有一些文件以一个数字结尾，这些是已轮循的归档文件。日志文件会变得特别大，特别笨重。Linux 提供了一个命令来轮循这些日志，以使你的当前日志信息不会淹没在旧的无关信息之中。logrotate 通常是定时自动运行的，但是也可以手工运行。当执行后，logrotate 将取得当前版本的日志文件，然后在这个文件名最后附加一个“.1”。其他更早轮循的文件为“.2”、“.3”，依此类推。文件名后的数字越大，日志就越旧。

（5）定制日志。可以通过编辑 /et/syslog.conf 和 /etc/sysconfig/syslog 来配置它们的行为，可以定制系统日志的存放路径和日志产生级别。

3. 系统各用户操作日志

单独执行 last 指令，它会读取位于/var/log 目录下名称为 wtmp 的文件，并把该文件的内容记录的登入系统中用户名单全部显示出来。

history 命令能够保存最近所执行的命令。如果是 root 命令所保存的命令内容在 /root/.bash_history 文件中，如果是普通用户，操作命令保存在这个用户的所属目录下，即一般的/home/username/.bash_history。这个 history 的保存值可以设置，编辑/etc /profile 文件，其中的 HISTSIZE=1000 的值就是 history 保存的值。

在平时，网络管理人员要经常提高警惕，随时注意各种可疑状况，并且按时检查各种系统日志文件，包括一般信息日志、网络连接日志、文件传输日志以及用户登录日志等。在检查这些日志时，要注意是否有不合常理的时间记载。例如：正常用户在半夜三更登录；不正常的日志记录，比如日志只记录了一半就切断了，或者整个日志文件被删除了；用户从陌生的网址进入系统；因密码错误或用户账号错误被摒弃在外的日志记录，尤其是那些一再连续尝试进入失败，但却有一定模式的试错法；非法使用或不正当使用超级用户权限 su 的指令；重新开机或重新启动各项服务的记录。

10.2.7　常用的安全工具

下面介绍一些可以用于 Linux 的安全工具，这些工具对于固化你的服务器将起到一定的作用，可以解决各方面的问题。

1. Sxid

Sxid 是一个系统监控程序。它可以监视系统中 suid、sgid 文件以及没有属主的变化，并且以可选的形式报告这些变化，你可以在配置文件中设置用 E-mail 的形式通知这些改变，也可以不使用 E-mail 而直接在标准输出上显示这些变化。suid、sgid 文件以及没有属主的文件很有可能是别人放置的后门程序，这些都是需要特别注意的。

缺省安装的时候，配置文件为/usr/local/etc/sxid.conf，这个文件中有很明显的注释，很容易看懂。在这个文件中定义了 Sxid 的工作方式。日志文件缺省为 /var/log/sxid.log，日志文件的循环次数在 sxid.conf 文件中定义。你可以在配置固定后把 sxid.conf 设置为不可改变，把 sxid.log 设置为只可添加（使用 chattr 命令）。

可以用 sxid -k 加上-k 选项来进行检查，这时检查很灵活，既不记入日志，也不会发出 E-mail，这样你就可以随时进行检查。

2. Sniffit

Sniffit 是一个有名的网络端口探测器，你可以配置它在后台运行以检测那些 Tcp/ip 端口上用户的输入/输出信息。

最常用的功能是攻击者可以用它来检测你的 23（Telnet）和 110（POP3）端口上的数据传送以便轻松得到你的登录口令和 mail 账号密码，Sniffit 基本上是被破坏者所利用的工具，但是既然想知道如何增强你的站点的安全性，首先你应该了解闯入者们所使用的各种工具。

安装是非常容易的，就在根目录运行#tarxvfzsniff*解开所有文件到对应目录。

可以运行 sniffit-i 以交互式图形界面查看所有在指定网络接口上的输入/输出信息。

3. Johntheripper

在 Linux 中，密码以 hash 格式被存储，你不能反向从该 hash 数据表中分析出密码，但可以以一组单词 hash 后和它进行比较，如相同则就猜测出密码。故起一个很难被猜测的密码是非常关键的。一般你决不能用字典存在的某个单词作为密码，那是相当容易被猜测出来的。另外也不能用一些常见的有规则性的字母数字排列来作为密码，以 123abc 等。

Johntheripper 是一个高效的易于使用的密码猜测程序，下载 tar.gz 格式的 forUNIX 的程序，然后用 tarxvfzjohn*.tar.gz 解开到任一目录下。进入 src 目录，输入 makelinux-x86-any-elf（我用 redhat6.1）后会在 run 目录下生成几个执行文件，包括主程序 john。现在要 Crack 密码就运行./john/etc/passwd 即可。

4. Logcheck

Logcheck 是用来自动检查系统安全入侵事件和非正常活动记录的工具，它分析各种 Linuxlog 文件，像/var/log/messages，/var/log/secure，/var/log/maillog 等，然后生成一个可能有安全问题的问题报告自动发送 E-mail 给管理员。你能设置它基于每小时，或者每天用 crond 来自动运行。

下载后用 tarxvfzlogcheck*解开到一临时目录如/tmp 下，然后用./makelinux 自动生成相应的文件到/usr/local/etc，/usr/local/bin/等目录下，你可能更改设置，如发送通知到谁的邮件账号，

默认发送到 root，你能设置 root 的邮件别名账号到一批人，更改设置让其忽略某些类型的消息，如你的邮件记录文件中的 plug-gw，因为 plug-gw 做反向 IP 查找，若找不到则记录一个警告消息到/var/log/maillog，Logcheck 默认记录下所有这些警告并发送给你，你可以通过设置忽略掉它们。

利用 Logcheck 工具分析所有 logfile，避免了每天经常手动地检查它们，节省了时间，提高了效率。

5. Tripwire

Tripwire 是一个用来检验文件完整性的非常有用的工具，你能定义哪些文件/目录需要被检验，不过默认设置能满足大多数的要求，它运行在 4 种模式下：数据库生成模式、数据库更新模式、文件完整性检查和互动式数据库更新。当初始化数据库生成的时候，它生成对现有文件的各种信息的数据库文件，万一以后你的系统文件或者各种配置文件被意外地改变，替换，删除，它将每天基于原始的数据库对现有文件进行比较，发现哪些文件被更改，你能根据 E-mail 的结果判断是否有系统入侵等意外事件。

6. PortSentry

PortSentry 是一个被设计成实时地发现端口扫描并对端口扫描快速作出反应的检测工具。一旦发现端口扫描，PortSentry 做出的反应有：

（1）通过 syslog()函数给出一个日志消息；

（2）自动地把对服务器进行端口扫描的主机加到 tcp wrappers 的/etc/hosts.deny 文件中；

（3）本地主机会自动把所有的信息流都重定向到一个不存在的主机；

（4）本地主机用包过滤程序把所有的数据包（来自对其进行端口扫描的主机）都过滤掉。

7. chkrootkit

chkrootkit 是设计用来检查许多广为人知的 rootkit（一组包括常用木马程序的套件，以方便 cracker 攻入主机时，在受害主机上顺利地编译和安装特洛伊木马程序）。在 chkrootkit 的网站上会公布最新的 rootkit 列表。

配置 chkrookit 非常简单：先从 http://www.chkrootkit.com 下载源代码，解开软件包，在文件被解开的路径里输入 make，完成后，chkrootkit 就随时侯命了。

（1）安装最新的系统补丁 Service Pack 与更新 HotFix 程序。微软公司会及时地将软件产品中发现的重大问题以安全公告的形式公布于众，这些公告都有一个唯一的编号。每个公告都有一个补丁程序，就是 HotFix，当 HotFix 累计到一定程度，微软就会以 SP（Service Pack）的方式把此前的 HotFix 整合起来。

（2）管理员账户的安全管理。

1）更改 Administrator 账户名

2）禁用 Administrator 账户

3）减少管理员组成员

4）系统管理员口令设置

（3）设置管理员账户密码时，应注意的问题。

第一，切不可让账号与密码相同。第二，切不可使用自己的姓名。第三，切不可使用英文词组。第四，切不可使用特定意义的日期。最后，切不可使用简单的密码。

（4）Windows 关闭不必要的服务。

1）关闭 IIS 服务。

2）关闭 NetMeeting 远程桌面共享服务。

3）关闭远程桌面帮助会话管理器服务。

4）关闭远程注册表服务。

5）关闭路由器和远程访问服务。

6）关闭简单文件共享（Simple File Sharing）服务。

7）关闭 SSDP 发现服务。

8）关闭 Telnet（远程登录）服务。

9）关闭 Universal Plug and Play Device Host 服务。

（5）拟定和实现一份审核策略时，应考虑和注意的因素。

1）明确所审核的类型和事件。常见的审计类型有 3 类：系统审计、应用程序审计和用户自行配置的安全性审计等。例如：用户的登录及登录退出、文件或目录的使用、关闭和重新启动 Windows NT Server、用户和组的改变以及安全规则的改变等。

2）明确审核的是事件的成功，还是失败的记录。

①跟踪事件的成功记录能了解文件和打印机的访问频率，从而有助于进行资源规划。

②跟踪事件的失败记录，将对非法入侵发出警报。

③在中等和高等安全的网络中，应该跟踪：用户登录成功和失败的记录，及资源的使用情况。

（6）文件权限管理。

1）通过共享许可（权限）保护网络资源

2）通过 NTFS 许可保护网络资源

（7）Linux 用户账号管理。

1）删除系统特殊的用户账号和组账号。

2）用户密码设置。

3）修改自动注销账号时间。

4）给系统的用户名密码存放文件加锁。

5）设定用户账号的安全等级。

6）限制超级用户的权力。

（8）网络和系统服务。

1）限制网络访问。NFS 访问；Inetd 设置；登录终端设置；避免显示系统和版本信息。

2）系统服务。关闭系统不使用的服务；给系统服务端口列表文件加锁；修改 ssh 服务的 root 登录权限。

（9）后台服务进程。

1）配置独立的专用服务器，增加负荷能力，降低风险。

2）取消所有非必要的服务，尽量做到干净，减少后门。

3）安全系数高的服务替代正在运行的服务进程。

4）使用 tcpwrappers 控制文件。

（10）日志系统。系统引导日志；系统运行日志；系统各用户操作日志。

（11）常用的安全工具。介绍一些可以用于 Linux 的安全工具：Sxid、Skey、Sniffit、Johntheripper、Logcheck、Tripwire、PortSentry、chkrootkit、secheck。

一、填空题

1．微软公司会及时地将软件产品中发现的重大问题以安全公告的形式公布于众，每个公告都有一个补丁程序，就是_____，当累计到一定程度，微软就会以_____的方式整合起来。

2．一条审核记录应该解决的问题和包含的内容：_____、_____、_____、_____、_____、_____。

3．安全审核系统将审核的结果保存在系统的各种日志中，包括_____、_____、_____。

4．共享目录许可的类型有 4 种，由高到低依次表示为：_____，_____，_____，_____。

5．Linux 防火墙包括两种类型：_____和_____。

二、选择题

1．（　　）是更改 Administrator 账户名。

A．更改本地计算机 Administrator 账户名

B．更改域 Administrator 账户名

C．更改网络 Administrator 账户名

D．通过组策略更改 Administrator 账户名

2．标准文件许可的类型有（　　）。

A．拒绝访问（None）　　B．读取（RX）

C．更改（RWXD）　　D．写入（W）

三、简答题

1．简述一下如何对管理员账户进行安全管理。

2．若欲保证账户密码的安全，应当遵循的规则？

3．通常情况下，在 Windows Server 2003 和 Windows Server 2008 网络中，对用户账户密码的要求是什么？

4．强密码具有哪些特征？

5．简述 Windows 需要关闭的不必要的服务。

6．Windows 系统可以审核哪些事件？

7．简述对于用户和组分配共享许可的一般准则。

8．简述应用和分配 NTFS 许可时的操作步骤。
9．简述如何对 Linux 用户账号进行管理。
10．如何去关闭 Linux 系统不使用的服务。
11．列举几个需要替代的进程。
12．如何对 SUID 和 SGID 攻击方式的预防。
13．列举几个常用的安全工具及其作用。