第 4 章　操作系统的安全

电子商务是一种基于网络的商务活动。网络是由各个不同的计算机系统组成的，而每个计算机系统的核心是操作系统。所以，计算机操作系统的安全是网络安全的基础，因而也是电子商务安全的一个重要组成部分。本节首先简要介绍涉及操作系统平台安全的一般性问题和原则，然后具体讨论目前几种最常用操作系统的安全特性，包括 UNIX/Linux 系统、Windows NT/2003 系统的一些安全问题。

4.1　操作系统安全性概述

操作系统作为计算机系统的基础软件是用来管理计算机资源的，它直接利用计算机硬件并为用户提供使用和编程接口。各种应用软件均建立在操作系统提供的系统软件平台之上，上层的应用软件要想获得运行的高可靠性和信息的完整性、保密性，必须依赖于操作系统提供的系统软件基础。在网络环境中，网络系统的安全性依赖于网络中各主机系统的安全性，而主机系统的安全性正是由其操作系统的安全性所决定的，没有安全的操作系统的支持，网络安全也毫无根基可言。所以操作系统安全是计算机网络系统安全的基础。

在安全层次模型中，操作系统的安全性属于系统级安全的范畴。操作系统为文件、目录、网络等提供底层的安全保障平台。操作系统中的安全缺陷和安全漏洞往往会造成严重的后果。因此，安全机制是操作系统的一个重要组成部分；平台的安全级别是对其性能进行评估的一个重要指标。本节简要地介绍一下操作系统安全服务的主要内容、安全性设计的主要原则，以及操作系统安全级别的划分。

4.1.1　操作系统安全性设计的原则

在操作系统平台的安全性设计方面，Saltzer 和 Schroeder 提出了一些基本原则：

（1）操作系统设计必须公开。认为入侵者由于不知道系统的工作原理而会减少入侵可能性的想法是错误的，这样只能迷惑管理者。

（2）默认情况应是拒绝访问。合法访问被拒绝的情况比未授权访问被允许的情况更容易获知。

（3）检查操作的当前授权信息。系统不应只检查访问是否允许，然后只根据第一次的检查结果而不理会后续的操作。

（4）为每个进程赋予可能的最小权限。每个进程只应当具备完成其特定功能的最小权限。

（5）保护机制必须简单、一致，并建立到系统底层。系统的安全性和系统的正确性一样，不应当是一种附加特性，必须建立到系统底层而成为系统固有的特性。

（6）方案必须是心理上可接受的。如果用户觉得为保护自己的文件而必须做这做那的话，用户就会有厌烦心理，并且可能因侥幸心理而不会利用所提供的方案保护数据。

4.1.2　操作系统的安全服务

操作系统的安全机制主要体现在身份认证和访问控制两个方面。身份认证要保证合法的

用户使用系统，防止非法侵入；访问控制则是要保证授权和受控地访问、使用系统资源。下面介绍操作系统安全服务的两个主要方面。

1. 用户管理的安全性

（1）用户账号的管理。通常对用户账号进行分组管理，并且这种分组管理应该是针对安全性问题而考虑的分组。也就是说，应该根据不同的安全级别将用户分为若干等级，每一等级的用户只能访问与其等级相对应的系统资源和数据，执行指定范围的程序。

（2）用户口令的加密机制。用户口令的加密算法必须有足够的安全强度，用户的口令存放必须安全，不能被轻易窃取。

（3）认证机制。身份认证必须强有力，即在用户登录时，与系统的交互过程必须有安全保护，不会被第三方干扰或截取。认证机制是用户安全管理的重点。用户身份认证通常采用账号/密码的方案。用户提供正确的账号和密码后，系统才能确认他的合法身份。不同的系统内部采用的认证机制和过程一般是不同的。

账号/密码的认证方案普遍存在着安全隐患和不足之处：

- 认证过程的安全保护不够健壮，登录的步骤没有做集成和封装，暴露在外，容易受到恶意入侵者或系统内特洛伊木马的干扰或截取。
- 密码的存放与访问没有严格的安全保护。比如，Linux 系统中全部用户信息，包括加密后的口令信息一般保存于/etc/passwd 文件中，而该文件的默认访问许可是任何用户均可读。因此，任何可能访问该文件副本的人，就有可能获得系统所有用户的列表，进而破译其密码。
- 认证机制与访问控制机制不能很好地相互配合和衔接，使得通过认证的合法用户进行有意或无意的非法操作的机会大大增加。例如能够物理上访问 Windows NT 机器的任何人，可能利用 NT Recover、Winternal Software 的 NT Locksmith 等工具程序来获得 Administrator 级别的访问权。

为此，Windows 2003 对身份认证机制做了重大的改进，引入了新的认证协议。Windows 2003 除了为向下兼容提供了对 NTLM 验证协议的支持以外（作为桌面平台使用时），还增加了 Kerberos V5 和 TLS 作为分布式的安全性协议，它支持对 Smart cards 的使用，这提供了在密码基础之上的一种交互式的登录。Smart cards 支持密码系统和对私有密钥及证书的安全存储。Kerberos 客户端的运行时刻是通过一个基于 SSPI 的安全性接口来实现的，客户 Kerberos 验证过程的初始化集成到了 WinLogon 单一登录的结构中。

2. 访问控制

访问控制是计算机保护中极其重要的一环，它是在身份识别的基础上，根据身份对提出的资源访问请求加以控制。在访问控制中，对其访问必须进行控制的资源称为客体，同理，必须控制它对客体的访问的活动资源称为主体。主体即访问的发起者，通常为进程、程序或用户。客体包括各种资源，如文件、设备、信号量等。访问控制中第三个元素是保护规则，它定义了主体与客体可能的相互作用途径。

访问控制实质上是对资源使用的限制，它决定主体是否被授权对客体执行某种操作。它通过鉴别使主体合法化，并将组成员关系和特权与主体联系起来。只有经授权的用户才允许访问特定的网络资源。

用户访问系统资源或执行程序时，系统应该先进行合法性检查，没有得到授权的用户访问或执行请求将被拒绝。系统还要对访问或执行的过程进行监控，防止用户越权。

程序的执行也应该受到监控。程序执行应遵循“最小”特权原则，程序不能越权调用执

行另外一些与本程序执行无关的程序，特别是某些重要的系统调用；也不能越权访问无关的重要资源。

系统中的访问控制通常通过定义对象保护域来实现。保护域是指一组（对象、权限）对，每个（对象、权限）对指定了一个对象以及能够在这个对象上执行的操作子集。保护域可以相互交叉。保护域规定了进程可以访问的资源。每一域定义了一组客体及可以对客体采取的操作。可对客体操作的能力称为访问权（Access Right），访问权定义为有序对的形式。一个域是访问权的集合。如域 X 有访问权，那在域 X 下运行的进程可对文件 A 执行读写，但不能执行任何其他的操作。

保护域并不是彼此独立的，它们可以有交叉，即它们可以共享权限。进程在执行过程中，可以根据情况在不同的保护域中切换，不同的系统对切换规则的定义不同。如图 4.1 所示，域 X 和域 Y 对打印机都有写的权限，发生访问权交叉。

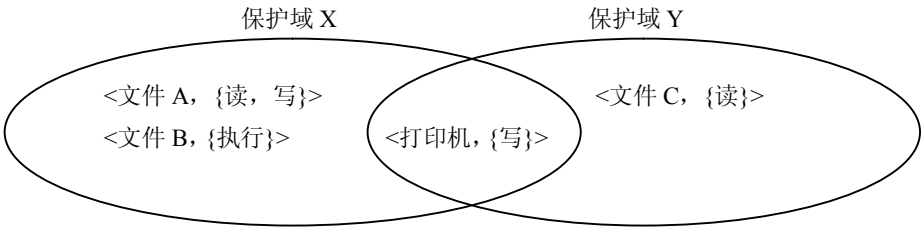

图 4.1　有重叠的保护域

一般客体的保护机制有两种：自主访问控制（Discretionary Access Control）和强制访问控制（Mandatory Access Control）。

所谓的自主访问控制是一种最为普遍的访问控制手段，用户可以按自己的意愿对系统的参数做适当修改以决定哪些用户可以访问他们的文件，亦即一个用户可以有选择地与其他用户共享他的文件。用户有自主的决定权。

所谓强制访问控制是指用户与文件都有一个固定的安全属性，系统用该安全属性来决定一个用户是否可以访问某个文件。安全属性是强制性的规定，它是由安全管理员或操作系统根据限定的规则确定的，用户或用户的程序不能加以修改。如果系统认为具有某一个安全属性的用户不适于访问某个文件，那么任何人（包括文件的拥有者）都无法使该用户具有访问该文件的权利。下面将分别介绍自主访问控制和强制访问控制。

（1）自主访问控制。一个安全的操作系统需要具备访问控制机制，它基于对主体及主体所属的主体组的识别来限制对客体的访问，还要校验主体对客体的访问请求是否符合存取控制规定来决定对客体访问的执行与否。这里所谓的自主访问控制，是指主体可以自主地 （也可能是单位方式）将访问权或访问权的某个子集授予其他主体。

为了实现完备的自主访问控制系统，由访问控制矩阵提供的信息必须以某种形式存放在系统中。访问矩阵中的每行表示一个主体，每一列则表示一个受保护的客体，而矩阵中的元素则表示主体可以对客体的访问模式。目前，在系统中访问控制矩阵本身都不是完整地存储起来，因为矩阵中的许多元素常常为空。空元素将会造成存储空间的浪费，而且查找某个元素会耗费很多时间。实际上常常是基于矩阵的行或列来表达访问控制信息。

（2）强制访问控制。自主访问控制是保护系统资源不被非法访问的一种有效手段，但是由于它的控制是自主的，所以也带来了问题。于是，人们又提出了一种更强有力的访问控制手

段，这就是强制访问控制。

在自主访问控制方式中，某一合法用户可以任意运行一程序来修改他拥有的文件存取控制信息，而操作系统无法区分这种修改是用户自己的操作还是恶意攻击的特洛伊木马的非法操作。

通过强加一些不可逾越的访问限制，系统可以防止某一些类型的特洛伊木马的攻击。在强制访问控制方式中，系统对主体和客体都分配一个特殊的安全属性，而且这一属性一般不能更改。系统通过比较主体和客体的安全属性来决定一个主体是否能够访问某个客体。用户的程序不能改变他自己及任何其他客体的安全属性。强制访问控制还可以阻止某个进程共享文件，并阻止通过一个共享文件向其他进程传递信息。

强制访问控制施加给用户自己客体的严格的限制，也使用户受到自己的限制。但是，系统为了防范特洛伊木马，必须要这么做。即便是不存在特洛伊木马，强制访问控制也有用，它可以防止在用户无意或不负责任的操作时，泄露机密信息。强制访问控制对专用的或简单的系统是有效的，但对通用、大型系统并不那么有效。一般强制访问控制采用以下几种方法：

1）限制访问控制。自主控制方式允许用户程序来修改他拥有文件的存取控制表，这为非法者带来可乘之机。因而，系统可以不提供这一方便。在这类系统中，用户要修改存取控制表的唯一途径是请求一个特权系统调用。该调用的功能是依据用户终端输入的信息，而不是靠另一个程序提供的信息来修改存取控制信息。

2）过程控制。在通常的计算机系统中，只要系统允许用户自己编程，就没办法杜绝特洛伊木马。但可以对其过程采取某些措施，这种方法称为过程控制。例如，警告用户不要运行系统目录以外的任何程序；提醒用户注意，如果偶然调用一个其他目录的文件时，不要做任何动作等。需要说明的一点是，这些限制取决于用户本身执行与否，因而自愿的限制很容易变成实际上没有限制。

3）系统限制。显然，实施的限制最好是由系统自动完成。要对系统的功能实施一些限制，比如限制共享文件，但共享文件是计算机系统的优点，所以是不可能加以完全限制的。再者，就是限制用户编程。事实上，有许多不需编程的系统都是这样做的。

不过这种做法只适用于某些专用系统。在大型的通用系统中，编程能力是不可能去除的；在网络中也不行，在网络中一个没有编程能力的系统可能会接收另一个具有编程能力的系统发出的程序。有编程能力的网络系统可以对进入系统的所有路径进行分析，并采取一定措施，这样就可以增加特洛伊木马攻击的难度。

4.1.3　操作系统安全级别的划分

信息安全产品和信息系统固有的敏感性及特殊性，直接影响着国家的安全利益和经济利益。因此，各国政府纷纷采取颁布标准、实行测评和认证制度等方式，对信息技术和安全产品的研制、生产、销售、使用及进出口实行严格、有效的管理与控制，并建立了与自身的信息化发展相适应的测评认证体系。

国外从 20 世纪 70 年代起就开展了建立安全保密准则的工作。美国国防部于 1983 年提出并于 1985 年批准的“可信任计算机标准评估准则”（TCSEC）为计算机安全产品的评测提供了测试准则和方法，指导信息安全产品的制造和应用，并做出了关于网络系统、数据库等的安全解释。由于 Internet 技术的广泛应用，信息系统的安全问题日益严重，新的问题也不断涌现。1992 年 12 月，美国颁布了新的联邦评测准则（K）来替代 80 年代颁布的 TCSEC 准则。 FC 中引入了“保护轮廓”（PP）这一重要概念，分级方式与 TCSEC 不同，每个轮廓都包括功能部分、开发保证部分和评测部分。

TCSEC 将计算机系统的安全可信性分为 7 个级别：

（l）D：最低安全性。

（2）C1：自主存取控制。

（3）C2：较完善的自主存取控制（DAC）、审计。

（4）Bl：强制存取控制（MAC）。

（5）B2：良好的结构化设计、形式化安全模型。

（6）B3：全面的访问控制、可信恢复。

（7）Al：形式化认证。

FC 充分突出“保护轮廓”，将评估过程分为“功能”和“保证”两部分，并将评估等级分为 EAL1～EAL7 共 7 级。每一级均需要评估 7 个功能类，即配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试、脆弱性评估。

就 TCSEC 评估来说，达到 B 级标准的操作系统即称为安全操作系统。在 B 级的安全计算机系统中，安全级这个概念包含级别和类别两方面。安全级的级别之间具有可比性，如同 2 级大于 1 级一样；而安全级的类别如同所属的部门，就像某人所属的单位，这个单位可大到整个跨国公司，也可小到所属的最小团体，甚至就是他本人。这样一种安全级定义，在计算机系统中就可以将一个用户定义成“属于哪几个部门的、级别为几的用户”，这就是该用户的安全级，凡是该用户运行的进程均具有这个安全级。同样，在计算机系统中也可以将一个文件（主页）定义成“属于哪几个部门的、级别为几的文件（主页）”，这就是该文件的安全级。 当用户的安全级与文件（主页）的安全级满足一定的存取控制规则时，该用户才可以对该文件（主页）进行相应的读写操作。这样，便实现了在计算机系统中对用户和文件（主页）的层次化分类管理。

目前，较流行的几种操作系统的安全性比较如表 4.1 所示。

表 4.1　几种操作系统的安全性比较

操作系统类型	安全级别
DOS	D
UNIX Ware2.1/ES	B2
Windows NT 4.0	C2
Windows 2000	C2
Solaris	C2

4.2　UNIX 系统的安全性

UNIX 是一种适用于多种硬件平台的多用户、多任务操作系统。最初的 UNIX 操作系统是 1969 年由美国 AT&T 公司贝尔实验开发出来的。从 1969 年至今，它经历了一个从开发、发展、不断演变和获得广泛应用，以至逐渐成为网络服务器和工作站的最重要的操作系统平台的过程。由于 Linux 是一种与 UNIX 安全兼容的操作系统，所以下面我们所讨论的 UNIX 系统的一般安全性问题基本上也适用于目前广泛流行的 Linux 系统。

4.2.1　口令与账号安全

用户账号和口令是系统安全的第一道防线。对入侵者来说，进入系统最直接的方法就是

获取用户账号和口令。由于有些用户账号和口令安全性差、比较脆弱，很容易被猜中，这给入侵者提供了可乘之机。本节主要阐述设置安全口令和账号的一些要点。

1. UNIX 登录认证机制

UNIX 的用户身份认证采用账号/口令的方案。用户提供正确的账号和口令后，系统才能确认他的合法身份。一般来说，通过终端登录 UNIX 系统的过程可描述如下：

（1）init 确保为每个终端连接（或虚拟终端）运行一个 getty 程序。

（2）getty 监听对应的终端并等待用户准备登录。

（3）getty 输出一条欢迎信息（保存在/etc/issue 中），并提示用户输入用户名，最后运行 login 程序。

（4）login 以用户作为参数，提示用户输入口令。

（5）如果用户名和口令相匹配，则 login 程序为该用户启动 shell；否则，login 程序退出，进程终止。

（6）init 程序注意到 login 进程已终止，则会再次为该终端启动 getty。

在上述过程中，唯一的新进程是 init 利用 fork 系统调用建立的过程，而 getty 和 login 仅仅利用 exec 系统调用替换了正在运行的进程。由于其后建立的进程均是由 shell 建立的子进程，这些子进程将继承 shell 的安全性属性，包括 uid 和 gid。

UNIX 在文本文件/etc/passwd（口令文件）中保存基本的用户数据库，其中列出了系统中的所有用户及其相关信息。在默认情况下，系统在该文件中保存加密后的口令。/etc/passwd 文件是 UNIX 安全的关键文件之一，该文件就用于在上述用户登录过程中校验用户的口令，它列出所有有效用户名及其相关信息。文件的每个用户一行，每行的一般格式为“LOG-NAME：PASSWORD：UID：GID：USERINFO：HOME：SHELL”，即每行包括用“：”分隔开 7 个域，其中每个域的含义如下：用户名、加密格式的口令、用户 ID、用户所在组的 ID、全名或账户的其他说明、用户主（home）目录、用户登录使用的 shell（登录时运行的程序）。

因为系统中的任何用户均可以读取/etc/passwd 文件的内容，因此所有人均可以读取任意一个用户的口令字段，即 passwd 文件每行的第二个字段。尽管口令是加密保存的，但是在现有黑客技术条件下，这种加密后的口令并不难以被黑客破译，尤其是简单的口令，更可以不花大量时间就可以破译。

为了加强安全，许多 UNIX 系统利用影像口令以避免在口令文件中保存加密的口令。它们将口令保存在单独的/etc/shadow 文件中，只有 root 才能读取该文件，而/etc/passwd 文件只在第二个字段中包含特殊的标记。

2. 口令安全

口令是账号安全最关键的部分。如果入侵者获得一个用户的口令，他就可以轻易地登录到系统上，并且拥有这个用户的所有权限。如果超级用户的口令被窃取，后果将不堪设想：入侵者控制了整个系统，他可以为所欲为，可以获取系统上的任何信息，还可以将系统随时摧毁。因此，选择一个安全的口令是非常必要的。

（1）选择安全的口令。一个好的口令应当至少有 6 个字符长，最好是大小写字母混合，并且口令中最好有一些非字母（如数字、标点符号、控制字符等），还要好记一些。选择口令的一个好方法是将两个不相关的词用一个数字或控制字符相连，并截断为 8 个字符。当然，如果你能记住 8 位乱码自然更好。另外，系统管理员一定要用 8 位口令，而且有~、！、@、#、$、%、<、>、*、&、?、:、”、｛、｝等符号。下面列出使用安全口令应该避免的几种情况：

1）使用用户名（账号）作为口令。 尽管这种方法在便于记忆上有着相当的优势，可是在安全上几乎不堪一击。几乎所有以破解口令为手段的黑客软件，都首先会将用户名作为口令的突破口，而破解这种口令几乎不需要时间。在一个用户数超过 1000 的计算机网络中，一般可以找到 10～20 个这样的用户。

2）使用用户名（账号）的变换形式作为口令。将用户名颠倒或者加前后缀作为口令，既容易记忆又可以防止许多黑客软件。不错，对于这种方法的确是有相当一部分黑客软件无用武之地，不过那只是一些初级的软件。 比如说著名的黑客软件 John，如果你的用户名是 fool，那么它在尝试使用 fool 作为口令之后，还会试着使用诸如 fool123、fooll、loof、loof123、lofo 等作为口令。只要是你想得到的变换方法，John 也会想得到，它破解这种口令，几乎也不需要时间。

3）使用自己或亲友的生日作为口令。这种口令有着很大的欺骗性，因为这样往往可以得到一个 6 位或 8 位的口令，但实际上可能的表达方式只有 100×12×31=37200 种，即使再考虑到年月日三者共有 6 种排列顺序，一共也只有 37200×6=223200 种。

4）使用常用的英文单词作为口令。这种方法比前几种方法要安全一些。如果你选用的单词是十分偏僻的，那么黑客软件就可能无能为力了。不过黑客多有一个很大的字典库，一般包含 10 万到 20 万的英文单词以及相应的组合。如果你不是研究英语的专家，那么你选择的英文单词恐怕十之八九可以在黑客的字典库中找到。如果是那样的话，以 20 万单词的字典库计算，再考虑到一些 DES（数据加密算法）的加密运算，每秒 1800 个的搜索速度也不过只需要 110 秒。

5）使用 5 位或 5 位以下的字符作为口令。从理论上来说，一个系统包括大小写、控制符等可以作为口令的一共有 95 个，5 位就是 7737809375 种可能性。使用 P200 破解虽说要多花些时间，但最多也只需要 53 个小时，可见 5 位的口令是很不可靠的。而 6 位口令也不过将破解的时间延长到一周左右。

（2）口令安全使用策略。选择安全的口令是非常必要的，但仅有这一点还远远不够。为进一步提高口令的安全性，还必须要求用户采用正确的使用策略。下面是安全使用口令需要注意的一些要点：

1）口令不能写在笔记本或书上，也不能存放在计算机上的某个文件中。因为无论是记在纸上还是存到文件中，它们的安全性都大大降低。所以把口令记在脑里才是最可靠、最安全的。

2）为防止眼明手快的人窃取口令，在输入口令时应确认无人在身边。

3）用户口令必须经常更换。一般来说，一个月或更短时间就必须更换一次口令，几个月甚至半年、一年都不换口令的用户是严重缺乏安全意识的。系统管理员应该定期通知、严格要求用户及时更改口令，以保证口令安全。

4）不应在不同机器中使用同一个口令，特别是在不同级别的用户上使用同一口令会引起全盘崩溃。

3. 账号安全

攻击都是从在系统中获得一个账号开始的。所以，设置安全账号、安全使用账号，是保证 UNIX 系统安全任务中最重要的一项工作。一般而言，保证账号安全要注意以下几个问题：

（1）谨慎使用 root 账号。root 用户在系统上拥有至高无上的权利，它可以读、写任何文件，运行任何程序。由于 root 用户可以完全控制整个系统，所以获得 root 用户的访问权限是“黑客”们的最高愿望。系统管理员应该记住：不要滥用 root 账号，只在必须的时候才使用 root 账号，而一般情况下应该使用普通用户账号。经常以 root 身份运行容易给入侵者带来可乘之机。

（2）经常更换账号口令。再安全的口令在经过一段时间后也会变得不安全，经常更换口令可以加强系统的安全性。然而，用户一般都很少更换口令，为此可以采用强制周期性更换口令的办法，防止因某一口令长期使用而引起的安全隐患。

（3）不要保留旧账号。一些规模庞大的 UNIX 系统可能具有许多旧账号，这些旧账号的用户可能已离开该组织或已搬迁到别的地方，账号长期没人使用，所以这类账号便成为了不安全的因素。为此，创建的账号应设置截止日期，若发现有超过截止日期的账号，可以同该用户联系，确定是否删除它。

（4）注意账号有效期。在拥有大量用户的系统中，经常有一些长期无人使用的账号。这些账号是系统潜在的安全漏洞，入侵者往往可以通过这些账号的不安全口令来攻击系统，而且由于账号长期无人使用，使得入侵者的攻击行为不易被及时发现。因此，系统管理员必须给每个账号设置使用期限。这个期限应该长短合适，既要能禁止废弃账号的使用，又要避免给用户带来不方便。账号期限可以在 passwd 文件中设置，然后可以使用 shell 脚本程序定期地检查每个账号的有效期。

对于临时出差、休假的用户，可暂时将他的账号禁用（用“*”号替换 passwd 文件中该账号的加密口令即可）。这样就可以防止其他人使用该账号，等该用户回来后，再把账号恢复。

（5）删除默认账号。许多 UNIX 系统中都设置默认账号，有时甚至存在默认口令或者没有口令的账号。所以，在刚安装完系统时，对这些默认账号要及时设置或更改口令或者直接删除。同时，不要随便设置组和组账号。

（6）guest 账号。为了方便外单位的临时用户，很多系统都提供了一个 guest 账号。 guest 账号是为短期使用系统的用户提供的，一般情况下很少使用。最安全的处理方法是，只在需要时才建立 guest 账号，等账号不再需要时，就立即把它从系统中删掉。不能把 guest 账号的口令设置得太简单，如 guest、visitor 等。

4.2.2　文件系统安全

1. UNIX 文件系统概述

UNIX 文件系统是 UNIX 系统的心脏部分，提供了层次结构的目录和文件。文件系统将磁盘空间划分为每 1024 个字节一组，称为 block（也有用 512 字节为一块的，如 SCOXENIX）。编号从 0 到整个磁盘的最大块数，全部块可划分为 4 个部分。块 0 称为引导块，文件系统不用该块；块 1 称为专用块，专用块含有许多信息，其中有磁盘大小和全部块的其他两部分的大小；从块 2 开始是 i 节点表，i 节点表中含有 i 节点，表的块数是可变的（后面将进行讨论）；i 节点表之后是空闲存储块（数据存储块），可用于存放文件内容。

文件的逻辑结构和物理结构是十分不同的，逻辑结构是用户敲入 cat 命令后所看到的文件，用户可得到表示文件内容的字符流；物理结构是文件实际上如何存放在磁盘上的存储格式。用户认为自己的文件是边界的字符流，但实际上文件可能并不是以边界的方式存放在磁盘上的，长于 1 块的文件通常将分散地存放在盘上。然而当用户存取文件时，UNIX 文件系统将以正确的顺序取各块，给用户提供文件的逻辑结构。

当然，在 UNIX 系统的某处一定会有一个表，告诉文件系统如何将物理结构转换为逻辑结构。这就涉及 i 节点了。i 节点是一个 64 字节长的表，含有有关一个文件的信息，其中有文件大小、文件所有者、文件存取许可方式，以及文件为普通文件、目录文件还是特别文件等。在 i 节点中最重要的一项是磁盘地址表。该表中有 13 个块号，前 10 个块号是文件前 10 块的存放地址。这 10 个块号能给出一个至多 10 块长的文件的逻辑结构，文件将以块号在磁盘地址

表中出现的顺序依次取相应的块。当文件长于 10 块时又怎样呢？磁盘地址表中的第 11 项给出一个块号，这个块号指出的块中含有 256 个块号，至此，这种方法满足了至多长于 266 块的文件（272384 字节）。如果文件大于 266 块，磁盘地址表的第 12 项给出一个块号，这个块号指出的块中含有 256 个块号，这 256 个块号的每一个块号又指出一块，块中含 256 个块号，这些块号才用于取得文件的内容。磁盘地址中和第 13 项索引寻址方式与第 12 项类似，只是多一级间接索引。这样，在 UNIX 系统中，文件的最大长度是 16842762 块，即 17246988288 字节。有幸的是 UNIX 系统对文件的最大长度（一般为 1～2MB）加了更实际的限制，使用户不会无意中建立一个用完整个磁盘所有块的文件。

文件系统将文件名转换为 i 节点的方法实际上相当简单。一个目录实际上是一个含有目录表的文件，对于目录中的每个文件，在目录表中有一个入口项，入口项中含有文件名和与文件相应的 i 节点号。当用户敲入 cat xxx 时，文件系统就在当前目录表中查找名为 xxx 的入口项，得到与文件 xxx 相应的 i 节点号，然后开始取含有文件 xxx 内容的块。

2. 文件许可权

文件属性决定了文件的被访问权限，即准能存取或执行该文件。用 ls-1 可以列出详细的文件信息，包括了文件许可、文件联结数、文件所有者名、文件相关组名、文件长度、上次存取日期和文件名。其中文件许可分为 3 部分，第一个 rwx 表示文件属主的访问权限；第二个 rwx 表示文件同组用户的访问权限；第三个 rwx 表示其他用户的访问权限。若某种许可被限制则相应的字母换为–。

在许可权限的执行许可位置上，可能是其他字母，如 s、S、t、T。s 和 S 可出现在所有者和同组用户许可模式位置上，与特殊的许可有关；t 和 T 可出现在其他用户的许可模式位置上，与“粘贴位”有关而与安全无关。小写字母（x、s、t）表示执行许可为允许，负号或大写字母（-、S 或 T）表示执行许可为不允许。

改变许可方式可使用 chmod 命令，并以新许可方式和该文件名为参数。新许可方式以 3 位八进制数给出，r 为 4，w 为 2，x 为 1。如 rwxr-xr-为 754。

改变文件的属主和组员可用 chown 和 chgrp，但修改后原属主和组员就无法修改回来了。

3. 目录许可权

在 UNIX 系统中，目录也是一个文件，用 ls-1 列出时，目录文件的属性前面带一个 d。目录许可也类似于文件许可，用 ls 列目录要有读许可，在目录中增删文件要有写许可，进入目录或将该目录作为路径分量时要有执行许可，故要使用任意一个文件，必须有该文件及找到该文件的路径上所有目录分量的相应许可。仅当要打开一个文件时，文件的许可才开始起作用，而 rm、mv 只要有目录的搜索和写许可，不需要文件的许可，这一点应注意。

4. 设备文件的安全考虑

UNIX 系统与系统上各种设备之间的通信通过特别文件即设备文件来实现。就程序而言，磁盘是文件，Modem 是文件，甚至内存也是文件。所有连接到系统上的设备都在/dev 目录中有一个文件与其对应。当在这些文件上执行 I/O 操作时，由 UNIX 系统将 I/O 操作转换成实际设备的动作。将设备处理成文件，使得 UNIX 程序独立于设备，即程序不必一定要了解正在使用的设备的任何特性，存取设备也不需要记录长度、块大小、传输速度、网络协议等这样一些信息，所有烦人的细节由设备驱动程序去关心考虑。要存取设备，程序只需打开设备文件，然后作为普通的 UNIX 文件来使用。

从安全的角度来看，上述处理方法很好，因为在任何设备上进行的 I/O 操作只经过了少量的渠道（即设备文件）。用户不能直接地存取设备，所以如果正确地设置了磁盘分区的存取许

可，用户就只能通过 UNIX 文件系统存取磁盘。文件系统有内部安全机制（文件许可）。

不幸的是，如果磁盘分区设置得不正确，任何用户都能够写一个程序读磁盘分区中的每个文件。其做法很简单：读 i 节点，然后以磁盘地址表中块号出现的顺序依次读这些块号指出的存有文件内容的块。故除了 root 以外，绝不要使磁盘分区对任何人可写。因为像所有者、文件存取许可方式这样一些信息存放于 i 节点中，任何人只要具有已安装分区的写许可，就能设置任何文件的 SUID 许可，而不管文件的所有者是谁，也不必用 chmod()命令，还可避过系统建立的安全检查。

以上所述对内存文件 mem、kmem 和交换文件 swap 也是一样的，这些文件含有用户信息，一个精心设计的程序可以将用户信息提取出来。要避免磁盘分区（以及其他设备）可读可写，应当在建立设备文件前先用 umask 命令设置文件，建立屏蔽值。不允许除 root 外的任何用户读或写盘分区的原则有一个例外，即一些程序（通常是数据库系统）要求对磁盘分区直接存取。解决这个问题的经验是磁盘分区应当由这种程序专用（不安装文件系统），而且应当告知使用这种程序的用户，文件安全保护将由程序自己而不是 UNIX 文件系统完成。

5. 安装和拆卸文件系统

UNIX 文件系统是可安装的，这意味着每个文件系统都可以连接到整个目录树的任意节点上（根目录总是被安装上的）。安装文件系统的目录称为安装点。/etc/mount 命令用于安装文件系统，用这条命令可将文件系统安装在现有目录结构的任意处。

安装文件系统时，安装点的文件和目录都是不可存取的，因此未安装文件系统时，不要将文件存入安装点目录。文件系统安装后，安装点的存取许可方式和所有者将改变为所安装的文件根目录的许可方式和所有者。

从安全的角度来讲，可安装系统的危险来自用户可能请求系统管理员为其安装用户自己的文件系统。如果安装了用户的文件系统，则应在允许用户存取文件系统前先扫描用户的文件系统，搜索 SUID/SGID 程序和设备文件。在除了 root 外，任何人不能执行目录中安装的文件系统，用 find 命令列出可疑文件，删除不属于用户所有的文件的 SUID/SGID 许可。用户的文件系统用完后，可用 umount 命令卸下文件系统，仅将安装点目录的所有者改回 root，存取许可改为 755。

6. 文件系统安全性检查

定期对文件系统安全性进行检查是保证系统安全的一个重要措施。检查内容包括：是否存在普通用户可以随意修改的文件、被授予过多权限的文件以及可以被入侵者访问的文件；是否出现一些陌生的新文件；配置文件是否被未授权用户修改等。

对文件系统安全性进行检查的一个常用工具是 find。该命令可以用文件名称、类型、存取权限、所有者、修改时间等选项来查找特定属性的文件。find 命令将搜索结果输出到屏幕或文件中。

4.2.3　系统管理员的安全策略

1. 加强系统管理员的安全意识

（1）保持系统管理员个人的登录安全。若系统管理员的登录口令泄密了，则窃密者离窃取 root 只有一步之遥。因为系统管理员经常作为 root 运行程序，如果窃密者非法进入到系统管理员的账户，将用特洛伊木马替换系统管理员的某些程序，毫不知情的系统管理员就会将这些已被替换的程序作为 root 运行。正是因为这个原因，在 UNIX 系统中，管理员的账户最容易受到攻击。系统管理员作为 root 运行程序时应当特别小心。下列一些指导规则可使系统管

理员保持个人登录安全：

1）不要作为 root 或以自己的登录账户运行其他用户的程序，首先用 su 命令进入用户的账户。

2）绝不要把当前工作目录放在 PATH 路径表的前边，那样实际是招引特洛伊木马。当系统管理员用 su 命令进入 root 时，他的 PATH 将会改变，就让 PATH 保持原样，以避免特洛伊木马的侵入。

3）敲入/bin/su 执行 su 命令。若有 su 源码，将其改成必须用全路径名运行（即 su 要确认 argv［0］的头一个字符是“/”才运行）。随着时间的推移，用户和管理员将养成敲入/bin/su 的习惯。

4）不要未注销账户就离开终端，特别是作为 root 用户时更不能这样。当系统管理员作为 root 用户时，命令提示符是“#”，这个提示符对某些人来说可能是个红灯标志。

5）不允许 root 在除控制台外的任何终端登录（这是 login 编译时的选项），如果有 login 源码，就将登录名 root 改成别的名，使破坏者不能在 root 登录名下猜测各种可能的口令，从而非法进入 root 的账户。

6）经常改变 root 的口令。

7）确认 su 命令记下的企图运行 su 的记录/usr/adm/sulog，该记录文件的许可方式是 600，并属 root 所有。这是非法者喜欢选择来替换成特洛伊木马的文件。

8）不要让某人作为 root 运行，哪怕是几分钟，即使有系统管理员在一旁注视着也不行。

（2）保持整个系统的安全。

1）保持账号安全。记录本系统的用户及其授权使用的系统；查出久未使用的登录户，并取消该账户；确保没有无口令的登录账户。

2）保持口令安全。

3）设置口令时效。如果能存取 UNIX 的源码，将加密口令和信息移到仅对 root 可读的文件中，并修改系统的口令处理子程序，这样可增加口令的安全性。修改 passwd，使 passwd 能删去口令打头和末尾的数字，然后根据 spell 词典和/etc/passwd 中用户的个人信息检查用户的新口令，也检查用户新口令中子串等于登录名的情况。如果新口令是 spell 词典中的单词，或/etc/passwd 中的入口项的某项值，或是登录名的子串，passwd 将不允许用户改变口令。

4）保持文件系统安全。检查所有系统文件的存取许可，任何具有 SUID 许可的程序都是非法者想偷换的选择对象；要特别注意设备文件的存取许可；要审查用户目录中具有系统 ID/系统小组的 SUID/SGID 许可的文件；在未检查用户的文件系统的 SUID/SGID 程序和设备文件之前，不要安装用户的文件系统；将磁盘的备份存放在安全的地方。

5）启动记账系统。

6）查出不寻常的系统使用情况，如大量地占用磁盘、大量地使用 CPU 时间、大量的进程、大量地使用 su 的企图、大量无效的登录、大量的到某一系统的网络传输、奇怪的 uucp 请求等。

7）修改 Shell，使其等待了一定时间而无任务时终止运行。

8）修改 login，使其打印出用户登录的最后时间，三次无效登录后，将通信线挂起，以便系统管理员能检查出是否有人试图非法进入系统。确保 login 不让 root 在除控制台外的任何地方登录。

9）修改 su，使得只有 root 能通过 su 进入某一户头。

10）当安装来源不可靠的软件时，要检查源码和 makefile 文件，查看特殊的子程序调用或命令。

2. 加强用户安全意识

UNIX 系统管理员的职责之一是保证用户安全，这其中一部分工作是由用户的管理部门来完成的，但是系统管理员作为系统运行的主要负责人，有责任发现和报告系统的安全问题。避免系统安全事故的方法是预防性的。当用户登录时，其 shell 在给出提示前先执行/etc/profile 文件，要确保该文件中的 PATH 指定最后搜索当前工作目录，这样将减少用户运行特洛伊木马的机会。

将文件建立屏蔽值的设置放在该文件中也是很合适的，可将其值设置成至少将防止用户无意中建立任何人都能写的文件。要小心选择此值，如果限制太严，用户很可能会在自己的.profile 中重新调用 umask 以抵制系统管理员的意愿。如果用户大量使用小组权限共享文件，系统管理员就一定要设置限制小组存取权限的屏蔽值。

系统管理员可每星期随机抽选一个用户，将读用户的安全检查结果（用户的登录情况简报、SUlD/SGID 文件列表等）发送给他的管理部门和他本人。这样做，主要有 4 个目的：

（1）大多数用户会收到至少有一个文件检查情况的邮件，这将引起用户考虑安全问题（虽然并不意味着用户们会采取加强安全的行动）。

（2）有大量可写文件的用户将一星期得到一次邮件，直到他们取消可写文件的写许可为止。冗长的邮件信息也许足以促使这些用户采取措施，删除文件的写许可。

（3）邮件将列出用户的 SUID 程序，引起用户注意自己有 SUID 程序，使用户知道是否有不是自己建立的 SUID 程序。

（4）送安全检查表可供用户管理自己的文件，并使用户知道对文件的管理关系到数据安全。如果系统管理员打算这样做，应事先让用户知道，以便他们了解安全检查邮件的目的。发送邮件是让用户具有安全意识，不要抱怨发送邮件。

管理意识是提高安全性的另一个重要因素。如果用户的管理部门对安全要求不强烈，系统管理员也可能忘记强化安全规则。最好让管理部门建立一套每个人都必须遵守的安全标准，如果系统管理员在此基础上再建立自己的安全规则就进一步强化。加强用户意识，让用户明确信息是有价值的资产。

系统管理员应当使安全保护方法对用户尽可能地简单，提供一些提高安全的工具，如公布锁终端的 lock 程序，让用户自己运行 secure 程序，将 pwexp（检查用户口令信息的程序）放入/etc/profile 中，使用户知道自己的口令时间。多教给用户一些关于系统安全的知识，确保用户知道自己的许可权限和 umask 命令的设置值。如果注意到用户在做错事，就给他们一些应当怎样做才对的提示。用户知道的关于安全的知识越多，系统管理员在保护用户利益方面做的事就越少。

4.3　Windows 系统的安全性

4.3.1　Windows NT 的安全性

1. Windows NT 的安全模型

在 Windows NT 最初的设计规格书中，安全性就已经包括并渗透在整个操作系统中了。在用户能对 Windows NT 的任一资源进行访问前，他们必须首先登录并被 Windows NT 所确认，且在工作站和服务器层次中都要求有确认机制工作。获得最初级的资源保护并不要求和 Windows NT 服务器连接，Windows NT 能提供这种本地安全性是因为每一台机器都有一个服

务器的账户和安全策略数据库的副本。这种安全机制包括控制谁能访问哪些对象（如文件和共享打印机），决定某人针对某一对象能做什么和什么事件被审计。

Windows NT 4.0 于 1999 年 11 月通过了美国国防部 TCSEC C2 级安全认证，它具有身份鉴别、自主访问控制、客体共享和安全审计等安全特性。为了支持这些安全特性，Windows NT 开发了专门的安全子系统。Windows NT 的安全子系统主要由本地安全授权（LSA）、安全账户管理（SAM）和安全参考监视器（SRM）等组成，如图 4.2 所示。

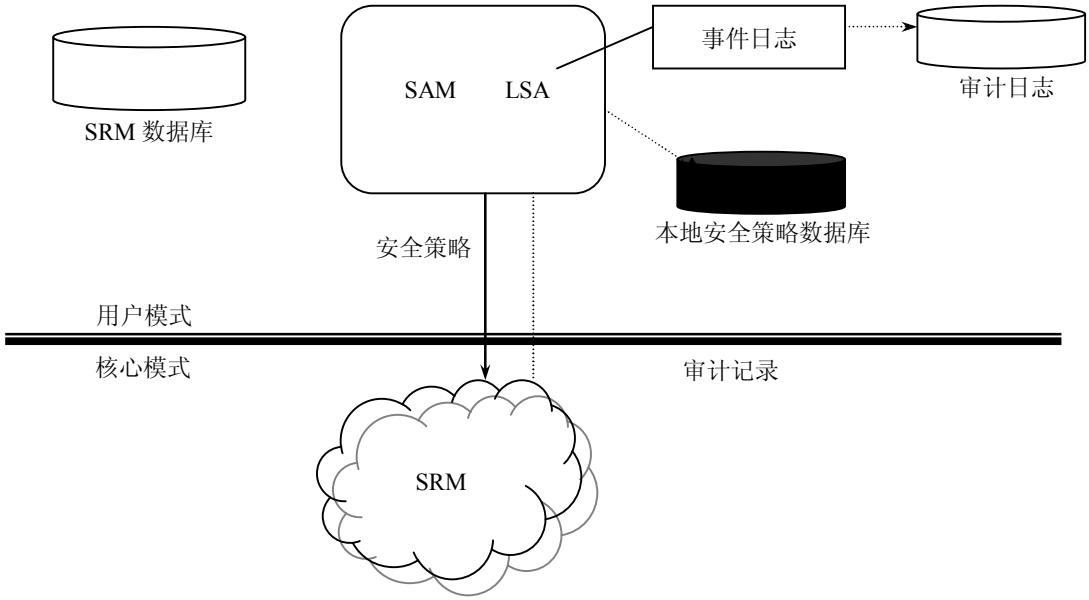

图 4.2 Windows NT 的安全子系统

（1）登录进程。登录进程可以进行 3 种类型的登录。如果某个用户退出之后再次登录回来，这个进程要取得用户的证明（用户名和口令），并且用安全账户管理器验证它。如果一个用户已经登录，而且试图访问另一个系统中的其他资源，这个进程就会验证到那个系统的用户。它还可以提供域间登录。

（2）本地安全授权（Local Security Authority，LSA）。本地安全授权部分提供了许多服务程序，保障用户获得存取系统的许可权。它产生令牌、执行本地安全管理、提供交互式登录认证服务、控制安全审查策略和由 SRM 产生的审查记录信息。

（3）安全账户管理（Security Account Manager，SAM）。安全账户管理部分保存 SAM 数据库，该数据库包含所有组和用户的信息。SAM 提供用户登录认证，负责对用户在 Welcome 对话框中输入的信息与 SAM 数据库中的信息比对，并为用户赋予一个安全标识符（SID）。根据网络配置的不同，SAM 数据库可能存在于一个或多个 Windows NT 系统中。

（4）安全参考监视器（Security Reference Monitor，SRM）。安全参考监视器负责访问控制和审查策略，由 LSA 支持。SRM 提供客体（文件、目录等）的存取权限，检查主体（用户账户等）的权限，产生必要的审查信息。客体的安全属性由安全控制项（ACE） 来描述，全部客体的 ACE 组成访问控制表（ACL）。没有 ACL 的客体意味着任何主题都可访问，而有 ACL 的客体则由 SRM 检查其中的每一项 ACE，从而决定主体的访问是否被允许。

Windows NT 的安全子系统是一个集成子系统，而不是环境子系统，因为它影响整个 Windows NT 操作系统。安全子系统的目标是保护系统的所有组件，包括硬件、软件和存储在

系统中的数据。Windows NT 操作系统中的任何东西都是对象，通过下面的方式控制对对象和系统的访问：

（1）Windows NT 根据附在每个对象上的访问控制列表（ACL）的定义控制谁能访问该对象，可以访问该对象的用户就对其拥有操作的“权限”（Permission）。

（2）当系统工作时，Windows NT 可控制用户的动作，这称为“权利”（Right）。系统管理员可以通过这些控制特别定义用户可以做什么和用户可以在哪里完成。操作系统可以通过这些控制保护对象免受非敌意的或恶意的重复使用与访问。

下面用标准《计算机信息系统安全保护等级划分准则》（GB 17895-1999）对 Microsoft Windows NT 4.0 操作系统（以下简称 Windows NT）的安全保护能力进行简单的分析。

（1）身份鉴别。Windows NT 有一个安全登录序列，用以防止不可信应用窃取用户名和口令序列，并有用户账号和口令等管理能力。

（2）自主访问控制。Windows NT 使用自主访问控制，其控制粒度达到单个用户。Windows NT 的安全模式允许用户将访问控制施用到所有的系统客体和使用 Windows NT 自有 NTFS 文件系统的全部文件。在应用或进程对任何客体打开一个句柄之前，Windows NT 安全系统透明地验证该进程所具有的相应授权，确保所有文件只有在文件的所有者或系统管理员的允许下，进程才能访问它。

（3）客体重用。在 Windows NT 的 TCB（Trusted Computing Base）接口，所有可见的资源都通过以下方式寻址：①在分配时清除客体；②在分配时完全初始化客体；③只允许已写入的部分被读取。

（4）审计。Windows NT 的 TCB 建立并维护有关身份鉴别、对所保护客体的访问、被保护客体的删除、管理行为以及其他与安全有关事件的一份记录。审计功能是由以下部件完成的：LSA、安全访问监控器 SRM、保护服务器与 Executive 子系统、Event Logger 和 EventViewer。审计信息记录在安全日志中，该日志只有在相应的“DAC 允许”取得之后才能被访问，或者拥有 SE-SECURITY-NAME 特权。只有管理员才被允许对安全日志进行访问。

2. Windows NT 4.0 的安全服务

（1）验证服务。Windows NT 4.0 要求在访问系统资源（如文件、目录等）以前进行验证。Windows NT 提供了一个引发安全性的键组合（Ctrl+Alt+Del 组合键）建立到操作系统的通信，而且也只到操作系统，以进行验证。这种信任路径机制的使用，可以防止特洛伊木马程序截获一个经过适当培训的用户的初始认证信息。

默认的验证机制是用户名和密码。Windows NT 提供了设置密码有效期限、强度（也就是长度）、历史，以及使用时间的能力。Windows NT 还针对可猜测性或者字典攻击提供了检测管理员密码的强度的密码过滤器。Windows NT 对存储在注册表中的密码信息进行了加密。这样的手段降低了对密码文件的基于字典的猜测式攻击，无论该文件是在本地机上还是攻击者把该文件复制到其他机器上。

Windows NT 把验证机制集成到全部安全操作和体系中。分布式应用程序使用 Windows NT 验证机制进行客户/服务器访问。这些验证机制使用挑战/响应协议，这个协议对密码进行数学转换，密码绝不会以明文形式传递。结合前面提到的很难被欺骗的信任路径登录，经过认真选择的用户密码是非常强大的。

（2）访问控制。Windows NT 提供两种形式的访问控制：对象许可和系统范围用户权利。对象许可，自由选择访问控制对象的创建者可以设置它们。用户权利，在分配给组的时候，允许一种基于角色的访问控制。Windows NT 的内核包括安全参考监视器（Security Reference

Monitor）在系统的一个单一模块上实现了这些访问仲裁控制。

在基于 Windows NT 的系统上的所有资源，例如文件（只有在 NTFS 上）、进程、打印机、注册表或者通信设备，在对象监视器中都用一个对象来表示。在一个对象上执行指定操作的许可存放在访问控制列表中（ACL，Access Control Lists）。ACL 提供了一个细粒度的访问控制，它们允许对象所有者基于独立用户或者它们定义的用户组以及管理员定义的组指定许可。为了管理上的方便，同时提供了本地组和全局组。关于 ACL，很重要的一点是它们是列表，因此所有者可以在一个对象上定义的规则的数量是没有限制的。这样，所有者可以指定一个非常全面的列表以完全实现他们希望实现的访问控制。

系统范围用户权利是一种赋予用户能力或权限来进行特定系统动作，而不会提供超出他们需要的权限的方法，它可以分别管理 27 种权限。这些权利和限制在登录的时候包含在验证过的用户名中，而且只能在用户被授予这种权限的时候才能改变（通常保留给网络管理员）。这意味着没有应用程序能为一般的用户修改他们自己的安全性设置，无论是偶然还是病毒侵袭。

（3）责任（Accountability）。Windows NT 紧密绑定一个安全 ID（SID，Security ID）。SID 唯一标识一个主机或域上的用户，它是同一次用户登录连接的进程相联系的访问记录的一部分，它自动成为系统产生的任何审核记录的一部分。该服务提供了所有的用户可以进行的动作的完整的责任——从文件访问到应用程序使用。跨越客户－服务器互动的责任由 Windows NT 客户－服务器访问验证维持。

（4）审核。Windows NT 提供了事件日志（Event Logging）。事件日志可以被配置在系统级别和对象级别，记录安全相关事件。系统事件包括登录和退出登录、文件和对象访问、用户权利的使用、用户和组管理、安全政策改变、重新启动和关机、系统错误，以及进程跟踪。文件和对象审核可以被控制在单个文件、目录，或者如果需要的话，也可以是驱动器。这些事件的组合足够满足可信任计算机安全评估标准（Trusted Computer Security Evaluation Criteria）的要求。

（5）安全分区。Windows NT 通过维护进程间的地址分离提供了进程孤立。实体间的所有访问和通信都通过仲裁接口。该仲裁是内核提供的，在一个用户编程不能使用的保护地址空间中操作。所有的内核功能包含在一个单一的模块中，即安全参考模块（Security Reference Module）。这样，把所有安全相关的功能集中到一个从一开始就为安全而设计的单一模块中。通过这个模块，Windows NT 内核控制任何应用程序可以访问的资源。例如，用一个普通用户的许可运行的应用程序不能访问其他应用程序，或者具有更高权限的用户保留的内存或者文件系统资源内核自动强制实现这个功能。

Windows NT 在分配系统缓冲给一个用户之前，会清除该缓冲并且维护一个文件使用指针以防止磁盘上文件块的重用，这样可以防止用户之间不可预测的信息流。另外， Windows NT 提供应用程序在返还交换空间给操作系统之前清除它们的能力，在系统关机的情况下也是一样。这些是很重要的存储空间重用功能，可以防止攻击者读取其他用户的应用程序留下的信息。

（6）完整性。Windows NT 使用 ACL 来防止对操作系统的访问。另外，Windows NT 具有一种数字签名操作系统代码的机制，可以检验它是否被修改过，以及确保它来自某个特定的作者或供应商。验证机制被用来保护通过互联网下载的应用程序，例如 ActiveX 控件或 Java。同样的机制还要用于操作系统代码。

Windows NT 提供了一个标准的加密接口（CAPI）以及 CSP 软件，可以被用来提供完整性服务以检验应用程序。深入到 Windows NT 文件系统（NTFS），容错磁盘驱动器可以同镜像组、复制组或有奇偶校验的数据条组共同使用，以保证写到磁盘上的信息的可用性。

（7）机密性。Windows NT 提供了一个标准的加密接口（CAPI）和软件加密服务提供者（CSP），可以被用于为广泛的产品提供加密。Windows NT 还提供了点对点隧道协议（PPTP）和安全套接字层（SSL），以保护通信中的数据。通信安全还可以使用基于互联网 IPSPEC 标准的第三方产品，Windows NT 通过安全 RPC 用分布式通信结构（DCOM）提供了对应用程序的保护。Windows NT 的验证协议避免了在网络登录和客户/服务器验证中以明文发送密码信息。

4.3.2　Windows 2003 的安全性

1. Windows 2003 的安全模型

Windows 2003 安全模型的主要功能是用户身份验证和访问控制。

（1）用户身份验证。Windows 2003 安全模型包括用户身份验证的概念，这种身份验证赋予用户登录系统访问网络资源的能力。在这种身份验证模型中，安全性系统提供了两种类型的身份验证：交互式登录（根据用户的本地计算机或 Active Directory 账户确认用户的身份）和网络身份验证（根据此用户试图访问的任何网络服务确认用户的身份）。为提供这种类型的身份验证，Windows 2003 安全系统包括了 3 种不同的身份验证机制：Kerberos V5、公钥证书和 NTLM（与 Windows NT 4.0 系统兼容）。

（2）基于对象的访问控制。通过用户身份验证，Windows 2003 允许管理员控制对网上资源或对象的访问。Windows 2003 通过允许管理员为存储在 Active Directory 中的对象分配安全描述符实现访问控制。安全描述符列出了允许访问对象的用户和组，以及分配给这些用户和组的特殊权限。安全描述符还指定了需要为对象审核的不同访问事件。文件、打印机和服务都是对象的实例。通过管理对象的属性，管理员可以设置权限、分配所有权以及监视用户访问。

管理员不仅可以控制对特殊对象的访问，也可以控制对该对象特定属性的访问。例如，通过适当配置对象的安全描述符，用户可以被允许访问一部分信息，如只访问员工姓名和电话号码而不能访问他们的家庭住址。

（3）Active Directory 和安全性。Active Directory 通过使用对象和用户凭据的访问控制提供了对用户账户和组信息的保护存储。由于 Active Directory 不仅存储用户凭据还存储访问控制信息，因此登录到网络的用户将同时获得访问系统资源的身份验证和授权。例如，用户登录到网络时，Windows 2003 安全系统通过存储在 Active Directory 上的信息来验证用户。然后，当用户试图访问网络上的服务时，系统检查由任意访问控制列表为这一服务定义的属性。由于 Active Directory 允许管理员创建组账户，因此管理员可以更有效地管理系统的安全性。例如，通过调节文件属性，管理员可以允许组中的所有用户读取文件。这样，访问 Active Directory 中的对象以组成员为基础。

Windows 2003 具有公共密钥加密基础架构。证书服务（Certificate Services）是通过密码保护的加密数据文件，其中包含的数据可用于对传输系统进行鉴别。证书服务可以分发、管理和撤消数字证书。基于公司的证书服务器可以用于客户机与服务器之间的相互认证，或者对不安全的连接中的数据进行加密，特别是对于 B to B 的电子商务。

Windows 2003 可以使用 IPSec 这种加密的 IP 协议来加密网络上的数据。同样，它可以在更高的传输层上使用 SSL 和更新的 TLS 规范来加密数据。在 Active Directory 中，这两种方式都可以被设置为强制性策略，以便特定的客户机和服务器之间能够进行通信。Windows 2003 的公共密钥加密是其 VPN 支持的基础。

但是该操作系统中最棒的加密措施是加密文件系统 （Encrypting File System，EFS），它允许你使用只有个别用户和经过认证的恢复代理能够解密的密钥对保存在磁盘上的文件进行加密。

EFS 改善了容易受到侵袭的系统（如笔记本电脑）的安全性。除非数据窃贼知道用户的密码，否则就不可能得到加密的数据。EFS 非常易于使用，加密不过是文件或文件夹的另一个属性。

总之，与传统版本的 Windows NT 系统相比，Windows 2003 系统采用了很多新的认证技术和协议，访问控制也设计得更加安全和灵活，网络和单个系统在 Windows 2003 下要远比 Windows NT 4.0 更加安全。

2. Windows 2003 的安全特性

正因为采用上述的安全机制，Windows 2003 实现了如下特性：数据安全性、企业间通信的安全性、企业和 Internet 的单点安全登录以及易用和良好扩展性的安全管理。

（1）数据安全性。Windows 2003 所提供的保证数据保密性和完整性的特性主要表现在以下 3 个方面：

1）用户登录时的安全性。从用户登录网络开始，Windows 2003 借助 Kerberos 和 PKI 等验证协议，提供了强有力的口令保护和单点登录。

2）网络数据的保护。本地网络中的数据是由验证协议来保证其安全性的。如果需要更高的安全性，还可以通过 IPSec 的方法提供点到点的数据加密安全性。

3）存储数据的保护。可以采用数字签名来签署软件产品（防范运行恶意的软件）或加密文件系统。加密文件系统基于 Windows 2003 中的 CryptoAPI 架构，实施 DES 加密算法，对每个文件都采用随机密钥来加密。加密文件系统不但可以加密本地的 NTFS 文件或文件夹，还可以加密远程的文件，不影响文件的输入输出。其恢复策略由 Windows 2003 的整体安全性策略决定，具有恢复权限的管理员才可以恢复数据，但是不能恢复用来加密的密钥。

（2）企业间通信的安全性。Windows 2003 为不同企业之间的通信提供了多种安全协议和用户模式的内置的集成支持，它的实现可以从以下 3 种方式中选择：

1）在目录服务中创建专门为外部企业开设的用户账号。通过 Windows 2003 的活动目录，可以设定组织单元、授权或虚拟专用网等方式，并对它们进行管理。

2）建立域之间的信任关系。用户可以在 Kerberos 或公用密钥体制得到验证之后，远程访问已经建立信任关系的域。

3）公用密钥体制。包括证书、智能卡和 PKI 证书可以用于提供用户身份确认和授权，企业可以把通过电子证书验证的外部用户映射为目录服务中的一个用户账号。Windows 2003 支持采用智能卡证书登录，同时还支持使用智能卡存储用于安全 E-mail 和其他与公用密码有关的证书，包括客户机验证、登录机制、代码签名和保护 E-mail。

（3）企业和 Internet 的单点安全登录。当用户成功地登录到网络之后，Windows 2003 透明地管理一个用户的安全属性，而不管这种安全属性是通过用户账号和用户组的权限规定（这是企业网的通常做法）来体现的，还是通过数字签名和电子证书（这是 Internet 的通常做法）来体现的。先进的应用服务器都应该能从用户登录时所使用的 SSPI 获得用户的安全属性，从而使用户做到单点登录，访问所有的服务。

（4）易用的管理性和高扩展性。通过在活动目录中使用组策略，管理员可以集中地把所需要的安全保护加强到某个容器（SDOU）的所有用户/计算机对象上。Windows 2003 包括了一些安全性模板，既可以针对计算机所担当的角色来实施，也可以作为创建定制的安全性模板的基础。

安全性管理的扩展性表现为，在活动目录中可以创建非常巨大的用户结构，用户可以根据需要访问目录中存储的所有信息，但是用户所在的域或组织单元仍然是安全性的边界，对访问的权限进行管制。

4.4　常见的操作系统安全漏洞

2000 年，SANS 研究所和国家基础设施保护中心（NIPC）发布了一份文档，总结了 10 个最严重的网络安全漏洞。数以千计的组织利用这份文档来安排他们工作的先后次序，以便能够首先关掉最危险的漏洞。2001 年 10 月 1 日，SANS 研究所发布了新的列表更新，同时扩展了以前的 TOP 10 列表，总结了 20 个最危险的安全漏洞，并将其分为三大类：通用漏洞、Windows 漏洞、UNIX 漏洞。

这份 SANS/FBI 最危险的 20 个漏洞列表是非常有价值的，因为大多数通过 Internet 对计算机系统的入侵均可以追溯到这 20 个安全漏洞。例如对五角大楼 Solar Sunrise 系统的攻击、Code Red 和 Nimda 蠕虫的快速传播，均可以归结为没有对这 20 个漏洞打补丁。

就是这少数几个软件漏洞成就了大多数的成功攻击，这是因为攻击者是机会主义者。他们使用最简单和常用的方法，并使用最有效和广泛传播的攻击工具，去攻击众所周知的漏洞。他们寄希望于有关组织不解决这些漏洞。他们扫描网络上有任何漏洞的系统，不做区分地加以攻击。

过去，系统管理员报告说他们没有弥补很多漏洞，是因为他们不知道哪些漏洞是最危险的，而且他们太忙了，没有时间修补全部漏洞。一些扫描工具可以扫描 300 个或 500 个，甚至 800 个漏洞，这就分散了系统管理员的注意力。系统管理员应该保障所有系统免于最常见的攻击。SANS/FBI 最危险的 20 个漏洞列表集合了大多数联邦安全机构、安全软件开发商、咨询公司、大学中的安全组织、CERT/CC 和 SANS 研究所的首席安全专家的知识，以简化以上问题。

4.4.1　影响所有系统的漏洞

1. 操作系统和应用软件的默认安装

大多数软件，包括操作系统和应用程序，都包括安装脚本或安装程序。这些安装程序的目的是尽快安装系统，在尽量减少管理员工作的情况下，激活尽可能多的功能。为实现这个目的，脚本通常安装了大多数用户所不需要的组件。软件开发商的逻辑是最好先激活还不需要的功能，而不是让用户在需要时再去安装额外的组件。这种方法尽管对用户很方便，但却产生了很多危险的安全漏洞，因为用户不会主动地给他们不使用的软件组件打补丁，而且很多用户根本不知道实际安装了什么。很多系统中留有安全漏洞就是因为用户根本不知道安装了这些程序。那些没有打补丁的服务为攻击者接管计算机铺平了道路。

对操作系统来说，默认安装几乎总是包括了额外的服务和相应的开放端口。攻击者通过这些端口侵入计算机系统。一般说来，你打开的端口越少，攻击者用来侵入你计算机的途径就越少。对于应用软件来说，默认安装包括了不必要的脚本范例，尤其对于 Web 服务器来说更是如此，攻击者利用这些脚本侵入系统，并获取他们感兴趣的信息。绝大多数情况下，被侵入系统的管理员根本不知道他们安装了这些脚本范例。这些脚本范例的安全问题是由于他们没有经历其他软件所必需的质量控制过程。事实上，这些脚本的编写水平极为低劣，经常忘记出错检查，给缓冲区溢出类型的攻击提供了“肥沃的土壤”。

（1）受影响的系统：大多数操作系统和应用程序。请注意，几乎所有的第三方 Web 服务器扩展都存在这样的样本文件，它们中间的大多数是极度危险的。

（2）如何判断是否易受攻击。如果用户使用了安装程序去安装系统或服务软件，而且没有移走不需要的服务或没有安装所有的安全补丁，那么其系统是易于被黑客攻击的。即使用户进行了附加的配置，也仍然是易受攻击的。用户应该对任何连到 Internet 上的系统进行端口扫

描和漏洞扫描。在分析结果时，请记住以下原则：用户的系统应该提供尽可能少的服务，并安装为提供这些服务所需的最少的软件包。每一个额外的软件或服务都为攻击者提供了一个攻击手段，这主要是由于系统管理员不会为他们不经常使用的软件打补丁。

（3）如何防范。卸载不必要的软件，关掉不需要的服务和额外的端口。这会是一个枯燥而且耗费时间的工作。正是由于这个原因，许多大型组织都为他们使用的所有操作系统和应用软件开发了标准安装指南。这些指南包括了为使系统有效运作所需的最少的系统特性的安装。

2. 没有口令或使用弱口令的账号

大多数系统都把口令作为第一层和唯一的防御线。用户的 ID 是很容易获得的，而且大多数公司都使用拨号的方法绕过防火墙。因此，如果攻击者能够确定一个账号名和密码，就能够进入网络。易猜的口令或默认口令是一个很严重的问题，但一个更严重的问题是有的账号根本没有口令。实际上，所有使用弱口令、默认口令和没有口令的账号都应从系统中清除。

另外，很多系统有内置的或默认的账号，这些账号在软件的安装过程中通常口令是不变的。攻击者通常查找这些账号。因此，所有内置的或默认的账号都应从系统中移出。

（1）受影响的系统：所有通过用户 ID 和口令进行认证的操作系统或应用程序。

（2）如何判断是否易受攻击。为判断是否易受攻击，用户需要了解自己的系统上都有哪些账号。应进行以下操作：①审计用户系统上的账号，建立一个使用者列表。别忘了检查例如路由、连接 Internet 的打印机、复印机和打印机控制器等系统的口令；②制定管理制度，规范增加账号的操作，及时移走不再使用的账号；③经常检查确认有没有增加新的账号，不使用的账号是否已被删除；④对所有的账号运行口令破解工具，以寻找弱口令或没有口令的账号；⑤当雇员或承包人离开公司时，或当账号不再需要时，应有严格的制度保证删除这些账号。

（3）如何防范。应采取两个步骤以消除口令漏洞。第一步，所有没有口令的账号应被删除或加上一个账号，所有弱口令应被加强。可悲的是，当用户被要求改变或加强他们的弱口令时，他们经常又选择一个容易猜测的。这就导致了第二步，用户的口令在被修改后，应加以确认。可以用程序来拒绝任何不符合安全策略的口令。

很多组织使用口令控制程序，以保证口令经常更改，而且旧口令不可重用。如果在使用口令有效期，请确认用户在口令过期之前收到警告并有足够的时间改变口令。当面对以下信息时“your password has expired and must be changed”，用户往往会选择一个坏口令。

Microsoft Windows 2003 在 Group Policy 中包括口令限制选项。系统管理员可以配置网络，使口令有最小长度、最小和最大有效期等限制。限制口令的最小有效期是很重要的，如果没有它，用户在被要求修改口令后会很快又把口令改回去。限制口令的最小有效期使得用户不得不记住现在的口令，而不太会把口令改回去。

另外一个很重要的手段是，使用户了解为什么以及怎样去选择强壮的口令。选择口令最常见的建议是选取一首歌中的一个短语或一句话，将这些短语的非数字单词的第一或第二个字母加上一些数字来组成口令。在口令中加入一些标点符号将使口令更难破解。另一个避免没有口令或弱口令的方法是采用其他认证手段，例如口令产生令牌（Password-generating tokens）或生物尺度（Biometrics）。如果你没有办法解决弱口令的问题，就尝试一下其他认证手段。

3. 没有备份或备份不完整

当事故发生时（这在每一个组织均有可能发生），从事故中恢复要求及时的备份和可靠的数据存储方式。一些组织的确每天都做备份，但是不去确认备份是否有效；其他一些组织建立了备份的策略和步骤，但却没有建立存储的策略和步骤。这些错误往往在黑客进入系统并已经破坏数据后才被发现。第二个问题是对备份介质的物理保护不够。备份保存了和服务器上同

样敏感的信息，它们应以相同的方式加以对待。

（1）受影响的系统：任何运行紧要任务的系统。

（2）如何判断是否易受攻击。应列出一份紧要系统的列表，然后对每一个系统可能遇到的风险和威胁进行分析。应根据这些重要的服务器制定备份方式和策略。一旦确认了这些重要系统，应明确以下重要问题：①系统是否有备份？②备份间隔是可接受的吗？③系统是按规定进行备份吗？④是否确认备份介质正确地保存了数据？⑤备份介质是否在室内得到了正确的保护？⑥是否在另一处还有操作系统和存储设施的备份（包括必要的 License Key）？⑦存储过程是否被测试及确认？

（3）如何防范。应当每天做备份。在大多数组织中，最低的要求是一周做一次完整的备份，之后每天再做增量备份。至少一个月要对备份介质做一次测试，以保证数据确实被正确地保存了下来。这是最低要求。

很多公司每天都做完整的备份，并且一天就要做多次备份。备份的终极目的是一个完全冗余的网络并且具备自动防故障能力，重要设施的控制系统和一些国防部门的系统都需要这样一个备份方案。

4. 大量打开的端口

合法的用户和攻击者都通过开放端口连接系统。端口开得越多，进入系统的途径就越多。因此，为使系统正常运作，保持尽量少的端口是十分必要的。所有无用的端口都应被关闭。

（1）受影响的系统：大多数操作系统。

（2）如何判断是否易受攻击。netstat 命令可以在本地运行以判断哪些端口是打开的，但更保险的方法是对用户的系统进行外部的端口扫描。这会列出所有实际在侦听的端口号。如果二者结果不同，用户应该研究一下是什么原因。如果两个列表一致，检查一下为什么这些端口是打开的，每一个端口都在运行什么。任何无法确认的端口都应被关闭。应记录最终端口列表，以确定没有额外的端口出现。

（3）如何防范。一旦用户确定了哪些端口是打开的，接下来的任务是确定所必须打开的端口的最小集合。关闭其他端口，找到这些端口对应的服务，并关闭/移走它们。

5. 没有过滤地址不正确的包

IP 地址欺诈是黑客经常用来隐藏自己踪迹的一种手段。例如常见的 smurf 攻击就利用了路由的特性向数以千计的机器发出了一串数据包，每一个数据包都假冒了一个受害主机的 IP 地址作为源地址，于是上千台主机会同时向这个受害的主机返回数据包，导致该主机或网络崩溃。对流进和流出网络的数据进行过滤可以提供一种高层的保护。过滤规则如下：①任何进入你网络的数据包不能把你网络内部的地址作为源地址；②任何进入你网络的数据包必须把你网络内部的地址作为目的地址；③任何离开你网络的数据包必须把你网络内部的地址作为源地址；④任何离开你网络的数据包不能把你网络内部的地址作为目的地址；⑤任何进入或离开你网络的数据包不能把一个私有地址（Private Address）或在 RFC1918 中列出的属于保留空间（包括 10.x.x.x/8、172.16.x.x/12 或 192.168.x.x/16 和网络回送地址 127.0.0.0/8）的地址作为源或目的地址；⑥阻塞任意源路由包或任何设置了 IP 选项的包。

（1）受影响的系统：大多数操作系统和网络设备。

（2）如何判断是否易受攻击。试图发送一个假冒 IP 地址的包，看自己的防火墙或路由器是否阻隔了它。用户的设备不仅应该阻隔它的传输，而且应该在日志文件中记录下假冒 IP 包已被丢弃。注意，这又为一种新的攻击敞开了大门——日志文件泛滥。应确认日志系统可以处理很强的负载，否则就易受 DOS 攻击。nmap 程序可以发出假冒 IP 包以测试这类过滤。一旦

设置了过滤规则，不要认为它总能正常工作，应经常测试。

（3）如何防范。应在外部路由或防火墙上设置过滤规则。以下是 Cisco 路由器的简单规则：

1）进入过滤：

```
interface    Serial 0
ip address 10.80.71.1 255.255.255.0
ip access-group ll in
access-list ll deny 192.168.0.0 0.0.255.255
access-list ll deny 172.16.0.0 0.15.255.255
access-list ll deny 10.0.0.0 0.255.255.255
access-list ll deny
access-list ll permit any
```

2）离开过滤：

```
interface    Ethernet     0
ip address 10.80.71.1 255.255.255.0
ip access-group ll in
access-list ll permit
```

6. 不存在或不完整的日志

安全领域的一句名言是：“预防是理想的，但检测是必须的。”只要你允许你的网络与 Internet 相连，黑客入侵的危险就是存在的。每周都会发现新的漏洞，而保护你不被黑客攻击的方法很少。一旦被攻击，没有日志，你会很难发现攻击者都做了什么。不了解这一点的话，你只能在两者之间做出选择：要么从原始状态重装系统，寄希望于数据备份是正确的，要么冒险使用一个黑客可能仍然控制的系统。

如果你不知道在你的系统上都发生了什么，你是不可能发现入侵的。日志提供了当前系统的细节，如哪些系统被攻击了、哪些系统被攻破了。

在所有重要的系统上应定期做日志，而且日志应被定期保存和备份，因为你不知何时会需要它。许多专家建议定期向一个中央日志服务器上发送所有日志，而这个服务器使用一次性写入的介质来保存数据，这样就避免了黑客篡改日志。

（1）受影响的系统：所有的操作系统和网络设备。

（2）如何判断是否易受攻击。查看每一个主要系统的日志，如果你没有日志或它们不能确定被保存了下来，那么你是易被攻击的。

（3）如何防范。所有系统都应在本地记录日志，并把日志发到一个远端系统保存。这提供了冗余和一个额外的安全保护层。现在两个日志可以互相比较。任何的不同显示了系统的异常。另外，这提供了日志文件的交叉检测。一个服务器中的一行日志可能并不可疑，但如果在一分钟内出现在一个组织的 50 个服务器的同一出口，可能标志着一个严重问题。

7. 易被攻击的 CGI 程序

大多数的 Web 服务器，包括 Microsoft 的 IIS 和 Apache，都支持 CGI 程序，以实现一些页面的交互功能，例如数据采集和确认。事实上，大多数 Web 服务器都安装了简单的 CGI 程序。不幸的是，大多数 CGI 程序员没有认识到他们的程序为 Internet 上的任意一个人提供了一个连向 Web 服务器操作系统的直接的链接。易被攻击的 CGI 程序格外吸引攻击者，是因为他们很容易确定和使用 Web 服务器上软件的权限。攻击者们可以利用 CGI 程序来修改 Web 页面，窃取信用卡账号，为未来的攻击设置后门。当司法部的页面被篡改后，深入调查得出的结论是：可能性最大的攻击

手段是 CGI 程序中的漏洞。由没有受过良好教育或很粗心的程序员编写的 Web 服务器应用程序也很容易受到攻击。作为一个基本的规则，所有系统都应删除示范（Sample）程序。

（1）受影响的系统：所有的 Web 服务器。

（2）如何判断是否易受攻击。如果你的 Web 服务器上有任何示范程序，那么你是易被攻击的。如果你有合法的 CGI 程序，请保证你是在运行最新版，然后对你的站点运行漏洞扫描工具。通过模仿攻击者的行为，你可以保护你的系统。你可以使用一个叫 whisker（http://www.wiretrip.net/rfp/）的 CGI 扫描工具来发现 CGI 程序的漏洞。

（3）如何防范。以下是为保护易受攻击的 CGI 程序所需做的首要工作：

- 从你的 Web 服务器上移走所有 CGI 示范程序。
- 审核剩余的 CGI 脚本，移走不安全的部分。
- 保证所有的 CGI 程序员在编写程序时都进行输入缓冲区长度检查。
- 为所有不能除去的漏洞打上补丁。
- 保证你的 CGI bin 目录下不包括任何的编译器或解释器。
- 从 CGI bin 目录下删除 view-source 脚本。
- 不要以 administrator 或 root 权限运行你的 Web 服务器。大多数的 Web 服务器可以配置成较低的权限，如 nobody。
- 不要在不需要 CGI 的 Web 服务器上配置 CGI 支持。

4.4.2　最危险的 Windows 系统漏洞

1．Unicode 漏洞

不论何种平台、何种程序、何种语言，Unicode 为每一个字符提供了一个独一无二的序号。Unicode 标准被包括 Microsoft 在内的很多软件开发商所采用。通过向 IIS 服务器发出一个包括非法 Unicode UTF-8 序列的 URL，攻击者可以迫使服务器逐字“进入或退出”目录并执行任意程序（Script——脚本），这种攻击被称为目录转换攻击。

Unicode 用%2f 和%5c 分别代表/和\，但你也可以用所谓的“超长”序列来代表这些字符。“超长”序列是非法的 Unicode 表示符，它们比实际代表这些字符的序列要长。/和\均可以用一个字节来表示。超长的表示法，例如用%c0%af 代表/用了两个字节。IIS 不对超长序列进行检查。这样在 URL 中加入一个超长的 Unicode 序列，就可以绕过 Microsoft 的安全检查。如果是在一个标记为可执行的文件夹中发出的请求，攻击者可以在服务器上运行可执行文件。更多的有关 Unicode 的威胁信息可在这里找到：http://www.wiretrip.net/rfp/p/doc.asp？id=57&face= 2。

（1）受影响的系统：安装了 IIS 4.0 的 Microsoft Windows NT 4.0 和安装了 IIS 5.0 而没有安装 Service Pack 2 的 Windows 2003 Server。

（2）如何判断是否易受攻击。如果你在运行一个未打补丁的 IIS，那么你是易受到攻击的。最好的判断方法是运行 hfnetchk。hfnetchk 是用来帮助管理员判断系统所打补丁情况的工具。Unicode 目录转换漏洞可通过打补丁进行修补。如果一个补丁都没有安装，那么系统是易受到攻击的。为进行进一步确认，你可以键入以下命令：http://victim/scripts/..%c0%af../winnt/system32/cmd.exe？/c+dir+c:\，这个地址需要被修改以准确测试每一个特定系统。如果你已移走了 scripts 目录（建议这么做），这个命令就失效了。你可以暂时建立一个有执行权限的目录或使用一个已有的有执行权限的目录来替代 Scripts 目录。例如，你可能已经删除了 scripts 目录，但另外有一个 cgi-bin 目录，可以使用 cgi-bin 目录替代 scripts 目录测试你的系统。

如果你是易受攻击的，这个 URL 会送回一个目录，列出驱动器 C 下的所有内容。以上的方法只是运行 DIR 命令，如果是一个攻击者的话，他就有可能使用该原理大肆破坏或在你的系统上安装一个后门。

（3）如何防范。为避免这一类攻击，你应下载 Microsoft 的最新补丁，在 Microsoft security Bulletin：http://www.microsoft.com/technet/security/bulletin/MS00-078.asp 你可以找到这些补丁的信息。

2. ISAPI 缓冲区扩展溢出

Microsoft Internet Information Server（IIS）是在大多数 Microsoft Windows NT 和 Windows 2003 服务器上使用的服务器软件。安装 IIS 后，就自动安装了多个 ISAPI Extensions。ISAPI 代表 Internet Services Application Programming Interface，允许开发人员使用 DLL 扩展 IIS 服务器的性能。 一些动态链接库，如 idq.dll，有编程错误，使得它们做不正确的边界检查。特别是，它们不阻塞超长字符串。攻击者可以利用这一点向 DLL 发送数据，造成缓冲区溢出，进而控制 IIS 服务器。

3. IIS RDS（Microsoft Remote Data Services）的使用

黑客可以利用 IIS Remote Data Services（RDS）中的漏洞以 administrator 权限在远端运行命令。

（1）受影响的系统：运行 IIS，有/msadc 虚拟路径的 Microsoft Windows NT 4.0 系统是最易受攻击的。

（2）如何判断是否易受攻击。如果你在运行一个未打补丁的系统，那么你是易被攻击的。可以在以下地址找到有关 RDS 漏洞和怎样清除它的指南：http://www.wiretrip.net/rfp/p/doc.asp？id=29&iface=2。

（3）如何防范。这不是仅打一个补丁就能修复的。为进行防范，请遵循以下安全公告（Security Bulletins）的指南：

- http://support.microsoft.com/support/kb/articles/q184/3/75.asp
- http://www. microsoft.com/technet/security/bulletin/ms98-004.asp
- http://www.microsoft.com/technet/security/bulletin/ms99-025.asp

另外，也可以通过升级到 2.1 版的 MDAC 来解决这个问题。最新版的 MDAC 可在以下地址获得：http://www.microsoft.com/data/download.htm。

4. NetBIOS——为保护的 Windows 网络共享

Server Message Blook（SMB）协议，也称为 Common Internet File System（CIFS），它允许网络间的文件共享。不正确的配置可能会导致系统文件的暴露或给予黑客完全的系统访问权。许多计算机所有者不知道他们在为了外来的研究人员或工作人员方便，而把文件设置为可读、可写后就为黑客们敞开了大门。

在 Windows 的主机上允许文件共享，使得它们容易受到信息窃贼和某种快速移动的病毒的攻击。在 Macintosh 和 UNIX 的主机上允许文件共享也存在相同的问题。

允许进行 Windows 文件共享的 Windows 机制可被攻击者利用获取系统的敏感信息。用户和组信息（用户名、上次登录时间、口令策略、RAS 信息）、系统信息和某种注册密钥都可通过与 NetBIOS 对话服务连接的一个“空对话”过程获得。这些信息对黑客很有帮助，因为这些信息可以帮助他们进行口令猜测和破解。

（1）受影响的系统：Microsoft Windows NT 和 Windows 2003。

（2）如何判断是否易受攻击。可在 Gibson Research Corporation 的网站 http://grc.com/进

行快速、免费安全的测试，以检查 SMB 文件共享和其他漏洞的存在。点击 ShieldsUP 图标可以检查是否存在 SMB 漏洞。注意，如果你所连接网络的某个中间器件阻塞了 SMB，ShieldsUP 会报告说你不存在这个漏洞，但事实上你可能存在漏洞。例如，对使用 Cable Modem 上网而供应商禁止 SMB 进入 Cable Modem 的用户，ShieldsUP 会报告说你不存在漏洞，但事实上，大约 4 千个和你使用同一个 Cable Modem 连接的用户均可使用这一漏洞。

Microsoft Personal Security Advisor 也可以判断你是否存在 SMB 漏洞并修复它。由于它是在本地运行，所以结果十分可靠。它可在以下网址获得：http://www.microsoft.com/technet/security/tools/mpsa.asp。

（3）如何防范。可采取以下手段防范：

- 在共享数据时，确保只共享所需目录。
- 为增加安全性，只对特定 IP 地址进行共享，因为 DNS 名可以欺诈。
- 对 Windows 系统（NT、2003），只允许特定用户访问共享文件夹。
- 对 Windows 系统，禁止通过“空对话”连接对用户、组、系统配置和注册密钥进行匿名列举。
- 对主机或路由器上的 NetBIOS 会话服务（TCP 139），Microsoft CIFS（TCP/UDP 445）禁止不绑定的连接。
- 考虑在独立或彼此不信任的环境下，在连接 Internet 的主机上部署 RestrictAnonymous Registry Key。可在以下网页找到更多信息：
  Windows NT 4.0：http://support.microsoft.com/support/kb/articles/Q143/4/74.asp。
  Windows 2003：http://support.microsoft.com/support/kb/articles/Q246/2/61.asp

5. 通过空对话连接造成的信息泄露

一个空对话连接（Null Session）也称为匿名登录，是一种允许匿名用户获取信息（例如用户名或共享文件）或不需认证进行连接的机制。explorer.exe 利用它来列举远程服务器上的共享文件。在 Windows NT 和 Windows 2003 系统下，许多本地服务是在 System 账号下运行的，又称为 Windows 2003 的 Local System。很多操作系统都使用 System 账号。当一台主机需要从另一台主机上获取系统信息时，System 账号会为另一台主机建立一个空对话。

System 账号实际拥有无限的权利，而且没有密码，所以你不能以 System 的方式登录。System 有时需要获取其他主机上的一些信息，例如可获取的共享资源和用户名等典型的网上邻居功能。由于它不能以用户名和口令进入，所以它使用空对话连接进入。不幸的是，攻击者也可以相同的方式进入。

（1）受影响的系统：Windows NT 4.0 和 Windows 2003。

（2）如何判断是否易受攻击。试用以下命令通过一个空对话连接到你自己的系统：net use\\a.b.c.d\ipc＄""/user:""（a.b.c.d 是远端系统的 IP 地址）。

如果你收到一个“connection failed”回复，你的系统就不存在这类漏洞，如果没有回复，就意味着以上命令执行成功，你的系统存在这类漏洞。

（3）如何防范。域控制器需要空对话进行通信。因此，如果你处在一个域的环境中，可以通过以下手段尽量减少攻击者所能获取的信息，但你永远不能消除所有泄露信息的手段：在 Windows NT 4.0 的主机上，修改以下注册表项：HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous=1。将 RestrlCtAnonymous 改为 1 仍然可使匿名信息。在 Windows 2000 下，可以把相应的值设为 2。这样做会使得在不允许外来的匿名用户（包括空对话用户）进行访问的时候，匿名用户不能获取任何信息。

修改注册表可能会造成系统工作不正常，因此必须事先进行测试。另外，所有系统应加以备份以便于恢复。如果不需要文件或打印机共享，可把 NetBIOS 从 TCP/IP 中解除。

注意这里在域控制器和其他主机上设置 RestricAnonymous 可能会影响网络的正常工作，因此建议只修改在 Internet 上可见的主机。其他主机都应受到可阻塞 NetBIOS 和 CIFS 的防火墙的保护。

Internet 用户应不能访问任何的域内控制器或其他不是用来提供外部访问服务的主机。为避免这类访问，关闭外部路由器或防火墙的以下端口：从 135 到 139 和 445 的 TCP、UDP 端口。

6. Weak、hashing in SAM（LM hash）

尽管 Windows 的大多数用户不需要 LAN Manager 的支持，微软还是在 Windows NT 和 2003 系统里默认安装了 LAN Manager 口令散列。由于 LAN Manager 使用的加密机制比微软现在的方法脆弱，LAN Manager 的口令能在很短的时间内被破解。即使是强健的口令散列也能在一个月内破解掉。LAN Manager 散列的主要脆弱性在于：①长的口令被截成 14 个字符；②短的口令被填补空格变成 14 个字符；③口令中所有的字符被转换成大写；④口令被分割成两个 7 个字符的片断。

这就意味着有口令破解程序只要破解两个 7 个字符的口令而且不用测试小写字符的情况。另外，LAN Manager 容易被侦听口令散列。侦听可以为攻击者提供用户的口令。

4.4.3 UNIX 系统漏洞

1. RPC 服务缓冲区溢出

远程请求（Remote Procedure Calls，RPC）允许一台机器上的程序执行另一台机器上的程序，它们被广泛地用来提供网络服务，如 NFS 文件共享和 NIS。由 RPC 缺陷导致的弱点正被广泛地利用着。有证据显示，1999 至 2000 年间的大部分分布式拒绝服务型攻击都是在那些通过 RPC 漏洞被劫持的机器上执行的。在 Solar Sunrise 事件中取得广泛成功的对美国军方系统的攻击，就是通过利用国防部几百个系统中的一个 RPC 缺陷来实现的。

（1）受影响的系统：UNIX 的大部分版本。

（2）如何判断是否易受攻击。检查你是否运行了下面 3 个被广泛利用的 RPC 服务中的一个：rpc.ttdbserverd、rpc.cmsd、rpc.statd。

这些服务通常被缓冲区溢出攻击成功利用，因为 RPC 程序不进行合适的错误检查。缓冲区溢出允许攻击者发送程序不支持的数据，因为程序不进行合理的错误检查，数据被继续传递和处理。

（3）如何防范。按照下面步骤保护你的系统避免该攻击：

- 只要允许，在可以从 Internet 直接访问的机器上关闭或删除这些服务。
- 在必须运行该服务的地方，安装最新的补丁：

Solaris software 补丁：http://sunsolve.sun.com/。

IBM AIX Software：http://techsupport.services.ibm.com/support/rs600O.support/downloads、http://techsupport.services.ibm.com/rs6k/fixes.html。

SGI Software 补丁：http://support.sgi.com/。

Compaq（Digital UNIX）补丁：http://www.compaq.com/support。

- 定期搜索供应商的补丁库，查找最新的补丁并立刻安装。
- 在路由或防火墙关闭 RPC 端口（Port 111）。
- 关闭 RPC loopback 端口 32770-32789（TCP 和 UDP）。

2. Sendmail 漏洞

Sendmail 是在 UNIX 和 Linux 上用得最多的发送、接收和转发电子邮件的程序。Sendmail 在 Internet 上的广泛应用使它成为攻击者的主要目标。过去的几年里发现了若干个缺陷。事实上，第一个建议是 CERT/CC 在 1988 年提出的，指出了 Sendmail 中一个易受攻击的脆弱性。其中最为常用的是攻击者可以发送一封特别的邮件消息给运行 Sendmail 的机器，Sendmail 会根据这条消息要求受劫持的机器把它的口令文件发给攻击者的机器（或者另一台受劫持的机器），这样口令就会被破解掉。

（1）受影响的系统：UNIX 和 Linux 的大部分版本。

（2）如何判断是否易受攻击。Sendmail 有很多易受攻击的弱点，必须定期地更新和打补丁。检查 Sendmail 最新版本和补丁版本，如果你没有更新版本或安装补丁文件，你可能就受此条影响。

（3）如何防范。应当采取下列步骤来保护 Sendmail：

1）更新 Sendmail 到最新版本或安装相应的补丁文件。http://www.cert.org/advisories/CA-97.05.sendmail.html。

2）在不是邮件服务器和代理服务器上，不要在 daemon 模式下（关闭 the-bd 开关）运行 Sendmail。

3. BIND 脆弱性

Berkeley Internet Name Domain（BIND）是域名服务 DNS（Domain Name Service）用得最多的软件包。DNS 非常重要，我们利用它在 Internet 上通过机器的名字（如 www.sans.org）找到机器而不必知道机器的 IP 地址。这使它成为攻击者钟爱的目标。令人悲哀的是，根据 1999 年中期的调查，连接在 Internet 上的 50%的 DNS 服务器运行的都是易受攻击的版本。在一个典型的 BIND 攻击的例子里，入侵者删除了系统日志并安装了工具来获取管理员的权限。然后他们编辑安装了 IRC 工具和网络扫描工具，扫描了 12 个 B 类网来寻找更多的易受攻击的 BIND。在一分钟左右的时间里，他们就使用已经控制的机器攻击了几百台远程的机器，并找到了更多的可以控制的机器。这个例子说明了像 DNS 这些无处不在的 Internet 服务软件中的一个单独的缺陷可能带来的一片混乱的局面。过期版本的 BIND 还存在缓冲区溢出的问题，攻击者可以用来获取未经授权的权限。

（1）受影响的系统：多个 UNIX 和 Linux 系统。

（2）如何判断是否易受攻击。运行漏洞扫描器检查 BIND 版本，或手工检查文件是否易受攻击。如果可疑（小心总不为过），就升级该系统。

（3）如何防范。应该采取下面步骤来防止 BIND 缺陷导致的攻击：

1）在所有 DNS 服务器的机器上，取消 BIND Name Daemon（称为 named）。有些专家建议删除 DNS 软件。

2）在被指定为 DNS 服务器的机器上升级到最新版本和补丁版本。采用下面的文章中的建议：

NXT 漏洞：http://www.cert.org/advisories/CA-99-14-bind.html。

QINV（Inverse Query）和 NAMED 漏洞：http://www.cert.org/advisories/CA-98.50.bindproblems.html、http://www.cert.org/summaries/CS-98.04.html。

3）以非特权的用户身份运行 BIND，以免远程控制的攻击。然而，DNS 要求只有作为 root 才有权配置 1024 以下的端口并运行该程序。因此，你必须配置 BIND 使其与端口捆绑后改变用户 ID。

4）在 chroot 目录下运行 BIND 以免受到远程控制攻击。

5）除了对授权的用户外，取消区域转换功能。

6）取消递规和粘合以保护 DNS 缓冲区位置。

7）隐藏版本字符串。

4. R 命令

在 UNIX 世界里，相互信任关系到处存在，特别是在系统管理方面。公司里经常指定一个管理员管理几十个区域甚至上百台机器。管理员经常使用信任关系和 UNIX 的 R 命令，从一个系统方便地切换到另一个系统。R 命令允许一个人登录远程机器而不必提供口令取代询问用户名和口令，远程机器认可来自可信赖 IP 地址的任何人。如果攻击者获得了可信任网络里的任何一台机器，他就能登录任何信任该 IP 的机器。下面的命令经常用到：

- rlogin：remote login，远程登录。
- rsh-remote shell：远程 shell。
- rcp：remote copy，远程拷贝。

（1）受影响的系统：UNIX，包括 Linux 的大部分版本。

（2）如何判断是否易受攻击。信任关系是通过设置两个文件来建立的，不是/etc/hosts.equiv 就是/etc/.rhosts。检查这些文件确认你的 UNIX 是否设置了信任关系。

（3）如何防范。不要允许以 IP 为基础的信任关系，不要使用 R 命令。基于 IP 地址的认证太容易被跳过，认证应该基于更安全的方式像 tokens 或者至少是口令。如果使用 R 命令，应限制它的登录范围，极其小心地控制可触及的网络的范围，永远不要把 rhost 文件放在 root 用户下。可以经常使用 UNIX 的 find 命令来查找由用户生成的任何 rhost 文件。

5. LPD

UNIX 里，in.LPD 为用户提供了与本地打印机交互的服务。LPD 侦听 TCP515 端口的请求。如果程序员在写代码时犯了一点错误，就会使得当打印工作从一台机器传到另一台机器时导致缓冲区溢出的漏洞。如果在较短的时间里接受了太多的任务，后台程序就会崩溃或者以更高的权限运行任意的代码。

（1）受影响的系统：Solaris 2.6 for SPARC、Solaris 2.6.x86、Solaris 7 for SPARC、Solaris 7 x86、Solaris 8 for SPARC、Solaris8 x86 和大多数 Linux 版本。

（2）如何判断是否易受攻击。可以对你的系统运行一个漏洞扫描程序来查找这个漏洞或者进行手工检查。最简单的办法是查看你的系统是否运行 LDP 以及它的版本。如果你使用的是该软件容易受攻击的版本并且没有打补丁，那么你的系统就将受到影响。

（3）如何防范。在受影响的机器上安装 Sun 公司提供的补丁文件。同时，还有其他的一些方法防止利用这个漏洞的攻击：

- 如果对远程的打印处理不是必要的，在/etc/inetd.conf 中关闭打印设备。
- 打开 noexec_user_stack，可以在/etc/system 文件里加入下面的行，然后重启来打开该功能：

set noexec_user_stack=l

set noexec_user_stack_log=l

- 限制到 port 515/tcp 的连接。
- 配置安装 tcpwrappers，它是 tcpd-7.6 软件包的一部分，可以从下面的地址下载：http://www.sun.com/solaris/freeware.html#cd。

6. Sadmind 和 Mountd

Sadmind 允许远程登录到 Solaris 系统进行管理，并提供了一个系统管理功能的图形用户

界面。Mountd 控制和判断在 UNIX 主机上的 NFS 的连接。由软件开发人员的错误导致的这些应用的缓冲区溢出漏洞，能被攻击者利用获取 root 的存取权限。

（1）受影响的系统：UNIX 的多个版本。

（2）如何判断是否易受攻击。使用漏洞扫描器查看这些服务是否在运行，以及它们是否易于被攻击。

（3）如何防范。下面的措施会防范 NFS 漏洞攻击，包括 Sadmind 和 Mountd：

- 只要有可能，在直接与 Internet 连接的机器上关闭或删除 Sadmind 和 Mountd。
- 安装最新的补丁：

Solaris Software Patches：http://sunsolve .sun.com/。

IBM AIX Software：http://techsupport.services.ibm.oom/support/rs6000.support/downloads、http://techsupport.services.ibm.com/rs6k/flixes.html。

SGI Sofiware Patches：http://support.sgi.com/。

Compaq（Digital UNIX）Patches：http://www.compaq.com/support。

- 使用基于 host/ip 的输出清单。
- 只要可能，把输出文件系统设置成只读或没有 suid。
- 使用 nfsbug 扫描漏洞。

可以在下面的地址找到更多的信息：http://www.cert.org/advisories/CA-99-16-sadmind.html、http://www.cert.org/advisories/CA-98.12.mountd.html。

7. 默认 SNMP 字串

SNMP（Simple Network Management Protocol，简单网络管理协议）是管理员广泛使用的协议，用来管理和监视各种各样与网络连接的设备，从路由器到打印机，再到计算机。SNMP 使用没有加密的公共字符串作为唯一的认证机制。没有加密已经够糟了，不仅如此，绝大部分 SNMP 设备使用的公共字符串还是 public，只有少部分“聪明”的设备供应商为了保护敏感信息，把字符串改为 private。攻击者可以利用这个 SNMP 中的漏洞，远程重新配置或关闭你的设备。被监听的 SNMP 通讯能泄漏很多关于网络结构的信息，以及连接在网络上的设备。入侵者可以使用这些信息找出目标和谋划他们的攻击。

（1）受影响的系统：所有的 UNIX 系统和网络设备。

（2）如何判断是否易受攻击。检查你的设备是否运行了 SNMP 协议，如果是，检查配置文件找到公共、漏洞：①默认的和空白的 SNMP community 名字；②容易猜测的 SNMP Community 名字。

（3）如何防范。下面的步骤会帮助抵御 SNMP 漏洞的攻击：

1）如果不是一定需要 SNMP，则关闭它。

2）如果一定要使用 SNMP，对社团号（Community Names）使用和口令一样的策略，确保它们难以猜测和破解，并定期改变。

3）使用 snmpwalk 命令验证和检验逆查社团号（Community Names）。可以在下面的链接中找到更多内容：http://www.zend.com/manualfunction.snmpwalk.php。

4）除非必须从本地网外部访问和管理设备，否则在边界路由器或防火墙处过滤掉 SNMP（Port161/UDP）。

5）只要可能，设置 MIB（管理信息结构）为只读。可以在以下地址找到更多信息：http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315。