第 3 章　操作系统安全基础及安全编程

本章学习要求：

- 了解各种 Windows 系统和 Linux 系统的安全机制。
- 掌握如何安装与配置 VMware 虚拟机。
- 了解网络协议分析器的工作原理。
- 掌握 Sniffer Pro 网络协议分析器的使用方法。
- 了解网络安全编程的相关知识。
- 掌握基本的网络安全编程方法。

3.1　操作系统安全

3.1.1　操作系统安全概述

操作系统是计算机资源的直接管理者，是连接计算机硬件与上层软件及用户的桥梁，是计算机软件的基础和核心，是计算机系统安全的基础，它的安全性至关重要。计算机操作系统的安全主要是利用安全手段防止操作系统本身被破坏，防止非法用户对计算机资源（如计算机硬件、系统应用软件、系统数据、系统控制等资源）的窃取。

操作系统的安全机制包括硬件安全机制、操作系统的安全标识和鉴别、访问控制、最小特权管理和可信通路等。

1. 硬件安全机制

安全操作系统的硬件安全机制，实质上也是普通操作系统所要求的，计算机硬件安全的目标是保证自身的可靠性和为系统提供基本安全机制。优秀的硬件保护性能是高效、可靠的操作系统的基础。硬件安全机制通常包括存储保护、运行保护、I/O 保护等。

存储保护是一个安全操作系统最基本的要求，主要是保护用户在存储器中的数据不受破坏。安全操作系统最重要的一点是实行分层设计，而运行域正是这样一种基于保护环的等级式结构。运行保护是指进程严格按照运行域机制运行。I/O 保护是操作系统功能中最复杂的一个功能，要寻找一个操作系统安全方面的缺陷，往往是从系统的 I/O 部分开始。一个安全的系统是把 I/O 赋予一个特权指令。用户程序要想启动 I/O，必须请求操作系统代为启动。

2. 操作系统的安全标识和鉴别

用户标识鉴别是操作系统提供的最外层保护措施。标识就是系统对每一个用户的身份都有一个特定的系统内部可以标识的标记，这个标记就是用户标识符。这个标识在全系统中是唯一的。将用户标识符与用户联系起来的过程就是鉴别。

3. 访问控制

操作系统的访问控制涉及自主访问控制和强制访问控制两个形式。自主访问控制是基于对主体或主体所属的主体组的识别,限制对客体的访问。自主访问控制技术有一个最主要的缺点,就是不能有效地抵抗计算机病毒的攻击。强制访问控制是"强加"给访问主体的,即系统强制主体服从访问控制策略。其主要特征是对所有主体及其所控制的客体(如:进程、文件、段、设备)实施强制访问控制。

4. 最小特权管理

所谓最小特权,指的是"在完成某种操作时所赋予网络中每个主体(用户或进程)必不可少的特权"。最小特权原则则是指"应限定网络中每个主体所必需的最小特权,确保可能的事故、错误、网络部件的篡改等原因造成的损失最小"。最小特权原则在安全操作系统中占据了非常重要的地位。角色管理机制是依据"最小特权"原则对系统管理员的特权进行的分化,每个用户只能拥有刚够完成工作的最小权限。

5. 可信通路

可信通路也是路径,是终端人员借以直接同可信计算机通信的一种机制,该机制只能由有关终端人员或可信计算机启动,并且不能被不可信软件所模仿。在用户执行一些操作时,用户必须确定是与安全核心通信而不是与一个特洛伊木马在交换信息。同时用户在进行特权操作时,也要有办法证实这是从内核输送出来的正确信息,不是来自特洛伊木马的模拟信息。这些都需要一个机制保障用户和内核的通信过程,这样的机制就是由可信通路提供的。

操作系统安全的实施将保护计算机硬件、软件和系统数据,防止人为因素造成的故障和破坏。因此,提高操作系统本身的安全等级尤为重要。它包括如下几个方面。

(1) 身份鉴别机制:实施强认证方法,比如数字证书等。

(2) 访问控制机制:实施细粒度的用户访问控制、细化访问权限等。

(3) 完整性:防止数据系统被恶意代码比如病毒破坏,对关键信息进行数字签名技术保护。

(4) 系统的可用性:不能访问的数据等于不存在,不能工作的业务进程毫无用处。因此还要加强应对攻击的能力,比如病毒防范、抵御黑客入侵等。

6. 审计

审计是一种有效的保护措施,它可以在一定程度上阻止对信息系统的威胁,并在系统监测、故障恢复等方面发挥重要的作用。

3.1.2 Windows 系统安全

Windows 系统是微软公司研究开发的操作系统,其发展经历了 Windows 3.1、Windows 98、Windows NT、Windows 2000、Windows XP、Windows 2003、Windows 2008 和 Windows Vista 等多个版本。由于 Windows 系统的易用性,许多用户都使用它,特别是其桌面操作系统。系统除了在操作方面的简单易用和稳定性外,其安全机制也是比较完善的。以下是 Windows 系统的安全机制介绍。

1. Windows 认证机制

早期 Windows 系统的认证机制不是很完善,甚至缺乏认证机制。如 Windows 3.x、

Windows 95/98 等。随着技术的进步，认证机制逐步完善。在 Windows 2000 中，系统就提供了两种认证方式，即本地认证和网络认证。

2. Windows 访问控制机制

Windows NT/XP 的安全性达到了橘皮书（可信计算机系统评测标准 TCSEC）C2 级，实现了用户级自主访问控制。其访问控制机制如图 3-1 所示。

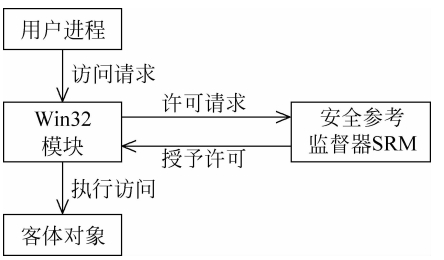

图 3-1　Windows 访问控制机制

3. Windows 审计/日志机制

日志文件是 Windows 系统中一个比较特殊的文件，它记录 Windows 系统运行状况，如各种系统服务的启动、运行和关闭等信息。Windows 系统日志有三种类型：系统日志、应用程序日志和安全日志，它们对应的文件名为 SysEvent.evt、AppEvent.evt 和 SecEvent.evt。这些日志文件通常存放在操作系统安装区域“system32\config”目录下。

4. Windows 协议过滤和防火墙

由于网络上的安全威胁日趋严重，Windows NT 4.0、Windows 2000、Windows 2003、Windows 2008 等均提供了包过滤机制，通过过滤机制可以限制网络中的数据包进入计算机。而 Windows XP 自带了防火墙，它能够实现监控和限制用户计算机的网络通信。

5. Windows 文件加密系统

为了防范入侵者通过物理途径读取磁盘信息，而不是通过 Windows 系统文件访问，Microsoft 开发了加密的文件系统 EFS，利用 EFS，文件中的数据在磁盘上是加密的。用户如果访问加密的文件，则必须拥有这个文件的 KEY，这个文件才能被打开，像其他普通文档一样。EFS 加密是基于公钥策略。被 EFS 加密过的数据不能在 Windows 中直接共享。如果通过网络传输经 EFS 加密过的数据，这些数据在网络上将会以明文的形式传输。NTFS 分区上保存的数据还可以被压缩，但是一个文件不能同时被压缩和加密。

虽然 Windows 系统已经有了一定的安全机制，但是各种各样的网络攻击仍层出不穷，考验着系统的安全与稳定。现在系统面临的主要威胁有以下几点。

（1）Windows 口令的安全。

（2）Windows 恶意代码。

（3）应用软件漏洞。

（4）系统程序的漏洞。

（5）注册表安全。

（6）文件共享安全。

（7）物理临近攻击。

针对这些威胁，Windows 系统提出了以下的安全增强方法。

（1）安全漏洞打补丁。由于很多漏洞本质上都是软件设计时的缺陷和错误，因此需要修复。

（2）停止服务和卸载软件。

（3）升级或更换程序。

(4) 修改配置或权限。

(5) 去除特洛伊木马等恶意程序。

(6) 安装可用的安全工具软件。

1. Windows NT 系统安全

Windows NT(New Technology)是微软公司第一个真正意义上的网络操作系统,它的发展经过 Windows NT 3.0/NT 4.0/NT 5.0(Windows 2000)和 Windows NT 6.0(Windows 2003)等众多版本,并逐步占据了广大中小网络操作系统的市场。

Windows NT 众多版本的操作系统使用了与 Windows 9x 完全一致的用户界面和完全相同的操作方法,使用户使用起来比较方便。与 Windows 9x 相比,Windows NT 的网络功能更加强大并且安全。

Windows NT 系列操作系统具有以下三方面的优点。

1) 支持多种网络协议

由于网络中可能存在多种客户机,这些客户机可能使用了不同的网络协议,如 TCP/IP、IPX/SPX 等。但 Windows NT 系统支持几乎所有常见的网络协议。

2) 内置 Internet 服务

随着互联网发展和 TCP/IP 协议簇的标准化,Windows NT 操作系统内置了 IIS,可以使用户轻松地配置各种网络服务。

3) 支持 NTFS 文件系统

Windows 9x 使用的文件系统是 FAT,在 NT 中内置同时支持 FAT 和 NTFS 的磁盘分区格式。FAT32 文件仅提供了文件夹的安全控制,而 NTFS 文件系统同时具备了安全性和稳定性,并且能设置文件和文件夹的安全性。全 32 位内核的 NTFS 为磁盘目录与文件提供安全设置,指定访问权限。NTFS 自动记录与文件相关的变动操作,具有文件修复能力。NTFS 文件系统每簇仅为 512B,硬盘利用率最高。但是 NTFS 也有自己不足的地方,它的兼容性差。NTFS 可以访问 FAT 文件系统,但是反向操作无法进行。目前支持 NTFS 分区格式的系统不多,除了 NT 外,Windows 2000、Windows XP、Windows 2003、Windows 2008 系统也支持这种文件系统形式。

2. Windows 2000 系统安全

Windows 2000 起初称为 Windows NT 5.0,它综合了 Windows 98 和 Windows NT 4.0 的很多优点和性能,Windows 2000 系统具有如下安全特性。

1) 活动目录

Windows 2000 Server 在 Windows NT Server 4.0 的基础上,进一步发展了活动目录(Active Directory)。活动目录是从一个数据存储开始的。它采用的是 Exchange Server 的数据存储,称为 Extensible Storage Service(ESS)。其特点是不需要事先定义数据库的参数,可以做到动态地增长,性能非常优良。活动目录包括两个方面:一个目录和与目录相关的服务。目录是存储各种对象的物理容器;而目录服务是使目录中的所有信息和资源发挥作用的服务。活动目录是一个分布式的目录服务。信息可以分散在多台不同的计算机上,保证快速访问和容错;同时用户可以在任何地方访问,为用户提供统一的视图。

2) 文件系统

Windows 2000 在 Windows NT Server 4.0R 高效文件服务基础上,加强和新增了分布

式文件系统、用户配额、加密文件系统、磁盘碎片整理和索引服务等服务。分布式文件系统帮助实现了不管文件的物理分布情况都把文件组织成树状的分层次逻辑结构，便于访问，加强了容错能力。Windows 2000 采用 NTFS 5 的文件系统，它改善了 NTFS 4 的访问许可权限。它增加了两个特别访问许可：权限改变和拥有所有权。Windows 2000 分布式网络环境中，增加了一个管理文件存储增长问题的新工具：磁盘配额。它允许管理员根据文件或文件夹的所有权来向用户分配磁盘空间，还可以设定警报和观察用户所剩的磁盘空间。加密文件系统是在磁盘上存储 NTFS 文件的一种新的加密存储方式。

3）存储服务

Windows 2000 中使用的存储管理体现在动态磁盘卷管理、磁盘碎片整理和自动系统恢复等方面。Windows 2000 还设计了通过层次性存储管理、支持新兴存储访问协议等方法来降低存储的成本。层次性存储管理是建立在远程存储服务之上的，能够不增加磁盘就可以在服务器上增加新的自由存储空间。

4）数据和通信安全

在数据和通信安全方面，Windows 2000 实现了如下的特征：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。Windows 2000 保证数据安全的方法通过以下三个方面实现：用户登录时的安全性，网络数据的保护，存储数据的保护。

虽然 Windows 2000 系统在安全方面又做了很大改进，但是仍然存在一些安全隐患，下面介绍一些增强系统安全的技术。

1）系统启动安全增强

非法用户若能以软盘及光盘启动计算机，那他就可以在 DOS 系统下随意对系统进行攻击。因此用户必须关闭软盘及光盘的启动功能。

2）账号与口令管理安全增强

在 Windows 2000 系统中用户账户有两种：活动目录用户账户和计算机账户。用户账户是用来记录用户的用户名和口令、隶属的组、可以访问的网络资源，以及用户的个人文件和设置。每个用户都应在域控制器中有一个用户账户，才能访问服务器，使用网络上的资源。用户账户由一个“用户名”和一个“口令”来标识，二者都需要用户在登录时输入。Windows 2000 提供可用于登录到 Windows 2000 计算机的预定义用户账户。账户通常分为两类：管理员账户和客户账户。每个预定义账户有不同的权利和权限组合，所以要合理使用和严格管理。计算机账户是指每个加入域的 Windows 2000 系统的计算机都应具有的账户。一个加入域的计算机账户，可拥有多个用户账户，且在不同的计算机上使用自己的用户账户进行网络登录。账号和口令经常成为入侵者入侵系统的突破口，账号越多，危险越大。因此要加强用户账号的管理。

加强用户账户管理的方法如下。

（1）停用 Guest 账户。在计算机管理的用户里面把 Guest 账户停用，任何时候都不允许 Guest 账户登录系统。

（2）限制不必要的用户数量。去掉所有的 duplicate user 账户。

（3）把系统 Administrator 账号改名。

（4）创建一个陷阱账号。创建一个 Administrator 的本地账号，把它的权限设为最低，

并设一个超复杂的口令。

(5) 设置安全复杂的口令。

(6) 设置屏幕保护口令。这是防止内部人员随意进入系统的一个屏障。

(7) 不让系统显示上次登录的用户名。

Windows 系统资源安全管理也是系统安全很重要的方面,可以通过下面的设置来提高系统的安全性。

(1) 共享权限的修改。在系统默认情况下,每建立一个新的共享,Everyone 用户就享有"完全控制"的共享权限,因此,在建立新的共享后应该立即修改 Everyone 的默认权限。

(2) 注册表安全。Windows 2000 中很多安全设置,都要通过注册表来进行,所以要保证注册表的安全。

对于 Windows 系统网络安全管理方面,可以通过下面的方法提高系统的安全性。

(1) 系统补丁。

(2) 禁止空连接。默认情况下,任何用户可以通过空连接连上服务器,进而枚举出账号,猜测口令。

(3) 关闭不必要的网络服务和网络端口。

过多的网络服务和端口的开放增加了系统的安全风险,为此应尽量避免打开不必要的服务和端口。

3. Windows Server 2003 系统安全

在 Windows 2000 基础上改进而来的 Windows 2003,因其操作方便,功能强大,成为一段时间内服务器操作系统的主流。在安全方面,Windows 2003 的安全模型发挥了巨大作用。

(1) Windows 2003 安全模型的功能

① 身份验证。Windows Server 2003 进行身份验证时分两部分执行:交互式登录和网络身份验证。

② 访问控制。访问控制是批准用户、组和计算机访问网络上的对象的过程。

③ 加密文件系统(EFS)。继续延续 Windows 2000 的这一技术,其对加密文件的用户是透明的,即此用户在使用该加密文件时不用手动解密。

④ 公钥基础结构。

⑤ Internet 协议安全性(IPSec)。它通过使用加密的安全服务以确保在 Internet 协议网络上进行保密和安全的通信。

(2) Windows Server 2003 中存在的安全问题

在安装的过程中,存在下面的安全隐患。

① 在接入网络时进行系统安装。因为在安装中,当输入 Administrator 密码后,系统就会自动建立 ADMIN$ 的共享。任何人都可以通过 ADMIN$ 进入系统。

② 操作系统与应用系统共用一个磁盘分区。当二者装在一个分区时,将导致一旦操作系统文件泄漏,攻击者可能获取应用系统的访问权限,从而影响应用系统的安全。

③ 采用默认安装。默认安装时可能会安装一些安全隐患的组件。

④ 系统补丁安装不及时,不全面。

在系统运行的过程中,仍然存在一些安全隐患。

① 默认共享：系统在运行后，会自动创建一些隐藏的共享。一般有以下几个共享文件：CDE$ 每一个分区的根共享目录；ADMIN$ 远程管理用的共享目录；IPC$ 空连接；NetLogon 共享。

② 默认服务：系统在运行后，自动启动了许多有安全隐患的服务，如 Telnet、Remote Registry Services 等，这些服务实际工作中如不需要，可以禁用。

③ 安全策略：默认下，安全策略是不起作用的。

④ 管理员账号：在系统运行后，Administrator 账号没有停用，攻击者可能一遍一遍尝试这个账号的口令。

⑤ 页面文件：页面文件用来存储没有装入内存的程序和数据文件部分的隐藏文件，其中可能含有敏感信息。

⑥ 共享文件：默认状态下，每个人对新创建的文件共享都拥有完全的控制权限，这是不安全的，应该严格控制用户的访问权限。

⑦ Dump 文件：Dump 文件在系统崩溃后和蓝屏的时候是一份很有用的查找问题的资料，但同时也会给攻击者提供一些敏感信息。

⑧ Web 服务：系统本身自带的 IIS 服务、FTP 服务存在安全隐患。

(3) 针对上面提到的安全隐患可以执行的安全防范措施

① 关闭系统默认共享。

方法 1：采用批处理文件在系统启动时自动删除共享。

方法 2：修改注册表，禁止默认的共享功能。

HKEY_LDCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameter 下新建一个双字节项 auto share server，设其值为 0 即可。

② 关闭不必要的服务。如 DHCP Client，DNS Client，Print spooler，Remote Registry Services，SNMP Services 等。

③ 启用安全策略。包括账号锁定策略，密码策略，审核策略，用户权限分配，安全选项。其中开启审核策略是系统最基本的入侵检测方法。下面的审核是必须开启的：审核系统登录事件、审核账户管理、审核登录事件、审核对象访问、审核策略更改、审核特权使用和审核系统事件。

④ 加强对 Administrator 账号和 Guest 账号的管理控制。

⑤ 清除页面文件。打开注册表，修改下面所示键的值：

HKEY_LDCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement 中的 ClearPageFileAtShutdown 的值改为 1，可以防止系统产生页面文件。

⑥ 清除 Dump 文件。打开“控制面板”→双击“系统”→打开“系统属性”→单击“高级”→单击“启动和故障恢复”选项区域中的“设置”→将“写入调试信息”改成“无”。

⑦ 防范 NetBIOS 漏洞攻击。关闭 139 服务端口。

⑧ 加强 IIS 服务器的安全。

4. Windows XP 系统安全

Windows XP 版本作为 Windows 系列中个人计算机用户的系统，具有运行可靠、稳定而且速度快的特点。成熟的技术支持，清新明快的外观设计，使用户有着良好的视觉享受。

个人用户使用的 Windows XP 包括专业版(Professional Edition)和家庭版(Home Edition)。两个版本基本相同,专业版只是额外增加了适用于企业网络用户和高级用户的特性。

Windows XP 继续延续 Windows 系列的安全机制,体现在安装安全策略、账号安全策略、应用安全策略、网络安全策略等方面。下面仅针对系统服务和进程的问题进行说明。

1) 完善的用户管理功能

Windows XP 采用 Windows 2000/NT 的内核,在用户管理上非常安全。凡是增加的用户都可以在登录的时候看到,不像 Windows 2000 那样,被黑客增加了一个管理员组的用户都发现不了。使用 NTFS 文件系统可以通过设置文件夹的安全选项来限制用户对文件夹的访问,如某普通用户访问另一个用户的文档时会提出警告。还可以对某个文件(或者文件夹)启用审核功能,将用户对该文件(或者文件夹)的访问情况记录到安全日志文件中,进一步加强对文件操作的监督。

拥有 Administrator 权限的用户,打开命令提示符窗口,输入"net start"命令后,就可看到已经开启的系统服务。如果为了详细查看,可以在"运行"里面输入"services. msc",打开服务设置窗口。服务分为三种启动类型:自动、手动、已禁用。

2) 透明的软件限制策略

在 Windows XP 中,软件限制策略以"透明"的方式来隔离和使用不可靠的、潜在的对用户数据有危害的代码,这可以保护用户的计算机免受各种通过电子邮件或网页传播的病毒、木马程序和蠕虫等的侵害,保证了数据的安全。

3) 支持 NTFS 文件系统以及加密文件系统

Windows XP 里的加密文件系统 (EFS)基于公众密钥,并利用 CryptoAPI 结构默认的 EFS 设置,EFS 还可以使用扩展的 Data Encryption Standard (DESX)和 Triple-DES (3DES) 作为加密算法。用户可以轻松地加密文件。

加密时,EFS 自动生成一个加密密钥。当用户加密一个文件夹时,文件夹内的所有文件和子文件夹都被自动加密了,数据就会更加安全。

4) 安全的网络访问特性

新的特性主要表现在以下几个方面。

(1) 补丁自动更新,为用户"减负"。

(2) 系统自带 Internet 连接防火墙。

自带了 Internet 防火墙,支持 LAN、VPN、拨号连接等。支持"自定义设置"以及"日志查看",为系统的安全筑起了一道"黑客防线"。

(3) 关闭"后门"。

在以前的版本中,Windows 系统留着几个"后门",如 137、138、139 等端口都是"敞开大门"的,在 Windows XP 中这些端口是关闭的。

5. Windows 7 系统安全

相对于 Windows XP 和 Vista,Windows 7 的性能有着显著的改进,但是它们的操作方式却极为相近。Windows 7 具有一个全新的、时髦的用户界面外观和许多的新功能,"尝试新鲜事物",这也是很多用户选择 Windows 7 的原因。

1) 保护内核

内核是操作系统的核心,这也使得它成为恶意软件和其他攻击的主要目标。如果攻击

者能够访问或操控操作系统的内核，那么他们可以在其他应用程序甚至操作系统本身都无法检测到的层次上执行恶意代码。微软开发了“内核模式保护”来保护核心，并确保不会出现未获授权的访问。

2）更安全的网页浏览

Windows 7 附带了功能更为强大的网页浏览器 IE8。用户也可以在其他的 Windows 操作系统版本上下载并运行 IE8，所以它不是专用于 Windows 7 的，但它确实带来了一些安全性能上的提升。

首先，InPrivate 浏览方式提供了私密上网的能力，就像 in private(私下地)这个名字它所揭示的一样。当启动一个 InPrivate 浏览窗口时，IE 浏览器不会保存个人网上冲浪的任何相关信息。这意味着，用户所输入的信息不会保存在 cache 中，也没有历史信息记录用户访问过的网站。当用户在一台共享或者公共的计算机上使用 IE8 时(比如在图书馆)，这项功能就显得特别有用。

IE8 另一个安全上的改进是保护模式。保护模式的实现是基于 Windows 7 的安全组件，这些组件能够确保恶意或未经授权的代码不会被允许在浏览器上运行。保护模式会阻止 drive-by 下载攻击，这些攻击使得用户在访问某个被攻破的网站时就能安装恶意软件到用户的系统中。

3）保护机制

用户账户控制(UAC)是 Windows Vista 上一个让所有人爱恨交织的。使用 Windows 7 时，UAC 仍然存在，但微软增加了一个控制滑杆，建议用户使用 UAC 提供的保护——这样就使弹出式对话框的数量受允许访问和执行文件数量的限制。

弹出对话框只是 UAC 所能做的能被看到的很小的一个方面。在 Windows Vista 下，许多用户只是简单地禁用全部 UAC，但那样也关闭了保护模式 IE 和一些其他的操作系统的保护。在 Windows 7 下的滑杆被默认设置为和 Windows Vista 相同的保护方式，但用户可以在控制面板下对它进行自定义设置。

4）安全工具和应用软件

Windows 防火墙和 Windows Defender 反间谍软件工具包含在 Windows 7 的基本安装包中。也可以下载并安装 Microsoft Security Essentials，这是一个微软发布的免费反病毒产品。

5）监控 Action Center

Windows XP 用户所熟悉的安全中心已被 Windows Action Center 所取代。Action Center 是一个包括安全中心的、更全面的监控 Windows 7 系统的控制台。

该 Action Center 的安全部分提供了用户 Windows 7 系统的涉及安全的粗略信息。建议随时对有关防火墙、间谍软件和病毒软件、Windows 的更新状态、Internet 安全设置和 UAC 的信息进行监控。

6. Windows Server 2008 系统安全

大多数的 Windows Server 2008 都同时拥有 32 位和 64 位两个版本，Windows Server 2008 for Itanium-based Systems 支持 IA-64 处理器。Windows Server 2008 是 Microsoft 最

后一个支持32位服务器的操作系统。下面是Windows Server 2008版本类型，它延续了Windows Server 2003的版本命名方式：

Windows Server 2008 Standard(简体中文正式零售标准版)

Windows Server 2008 Enterprise(简体中文正式企业版)

Windows Server 2008 Datacenter (简体中文正式数据中心版)

Windows Web Server 2008(简体中文正式网站服务器版)

Windows Server 2008 for Itanium-Based Systems(简体中文正式安腾版)

Windows Server 2008的主要特点如下。

1) Server Core

作为服务器操作系统，Windows Server一直以来颇为诟病的地方就是，它是“Windows”，因为管理员根本不需要安装图书驱动、DirectX、ADO、OLE等东西，毕竟他们不需要运行用户程序；而且，图形用户界面一直是影响Windows稳定性的重要因素，精简了的图形用户界面可以减少内存资源占用，增强稳定性和安全性。

Windows Server 2008当中最引人注意的地方是它崭新的安装模式，在安装时必须允许服务器的管理员选择安装整个服务器软件，或者只安装“服务器核心(Server Core)”。

“服务器核心”是一种恢复到从前的安装方式，没有图形用户界面(GUI)，所有的设置与维护都是由命令控制，或者是利用Microsoft Management Console进行远程联机操作。“服务器核心”同时也不会内置Internet Explorer等其他许多与核心服务不相干的功能。

2) PowerShell

PowerShell原计划作为Windows Vista的一部分，但只是作为免费下载的增强附件，随后又成了Exchange Server 2007的关键组件，后来又被集成到Windows Server 2008中。这个新的命令行工具可以作为图形用户界面管理的补充，也可以彻底取代它。

3) 虚拟化

以往在企业级虚拟化领域，VMware的ESX Server、Citrix的XenServer等平台受关注的程度几乎很高。Hyper-V是微软伴随Windows Server 2008最新推出的服务器虚拟化解决方案，与微软自家的Virtual PC、Virtual Server等产品相比，有着很显著的区别。与Virtual Server要经过三层的转换相比，Hyper-V的基本架构简化了虚拟机和硬件之间的层数，这种架构使得虚拟机和硬件之间只通过很薄的一层进行连接，因而虚拟机执行效率非常高，可以更加充分地利用硬件资源，使虚拟机系统性能非常接近真实的操作系统性能。

4) Internet Information Server(IIS) 7.0

Internet Information Server(IIS) 7.0支持以FastCGI方式运行PHP，与Windows Server 2003(IIS 6.0)和Windows 2000(IIS 5.0)相比有很大的提高。

3.1.3 Linux系统安全

随着Internet/Intranet的日益普及，采用Linux网络操作系统作为服务器的用户也越来越多，这一方面是因为Linux是开放源代码的免费正版软件，另一方面也是因为较之微软