高等学校计算机科学与技术教材

网络操作系统安全

杨富国　主编
叶传标　任吉治　编
周惠民　乔正洪

清 华 大 学 出 版 社
北京交通大学出版社
·北京·

内 容 简 介

本书从安全角度出发，理论联系实际，重点介绍 Windows 类和 UNIX 类网络操作系统的安全设置和管理技巧，可操作性和实用性很强。通过本书的学习，不仅可以深刻理解网络操作系统的安全机制，而且可以掌握常用网络操作系统的安全配置方法和安全管理技巧。

本书以网络安全管理人员为主要读者对象，同时兼顾广大计算机网络爱好者的需求，是一本进行网络操作系统安全设置和管理的实用教材和必备参考书。

图书在版编目（CIP）数据

网络操作系统安全 / 杨富国主编. — 北京：清华大学出版社；北京交通大学出版社，2005.10
（高等学校计算机科学与技术教材）
ISBN 7－81082－614－X

Ⅰ. 网…　Ⅱ. 杨…　Ⅲ. 计算机网络-操作系统（软件）-安全技术-高等学校-教材
Ⅳ. TP316.8

中国版本图书馆 CIP 数据核字（2005）第 100923 号

责任编辑：张利军
出 版 者：清华大学出版社　邮编：100084　电话：010－62776969　http：//www.tup.com.cn
　　北京交通大学出版社　邮编：100044　电话：010－51686414　http：//press.bjtu.edu.cn
印 刷 者：北京鑫海金澳胶印有限公司
发 行 者：新华书店总店北京发行所
开　本：185×260　印张：23　字数：590 千字
版　次：2005 年 10 月第 1 版　2005 年 10 月第 1 次印刷
书　号：ISBN 7－81082－614－X/TP・230
印　数：1～4 000 册　定价：30.00 元

编　委　会

前　言

操作系统是计算机资源的直接管理者，是计算机软件的基础和核心，一切应用软件都是建立在操作系统之上的，如果没有操作系统的安全，就谈不上主机和网络系统的安全，更谈不上其他应用软件的安全。因此，操作系统的安全是整个计算机系统安全的基础。

与过去相比，如今的操作系统性能更先进、功能更丰富，但同时也增加了安全漏洞。要想减少操作系统的安全漏洞，需要对操作系统予以合理配置、管理和监控。通常的安全入侵事件，多数都归因于操作系统没有合理配置，或者没有经常核查及监控。操作系统都是以默认安全设置来配置的，因而，极容易受到攻击。

本书从安全角度出发，以理论为指导，重点介绍网络操作系统的安全设置。通过阅读本书，不仅可以深刻理解目前最为流行的 Windows 类和 UNIX 类网络操作系统的安全机制，而且可以掌握常用网络操作系统的安全配置方法和安全管理技巧。

本书注重所述内容的可操作性和实用性，以网络安全管理人员为主要读者群体，同时兼顾广大计算机网络爱好者的需求，是一本进行网络操作系统安全管理的实用教材和必备的重要参考书。

本书的组织结构

本书把目前最为流行的网络操作系统分为两个部分，上篇第 1～8 章介绍 Windows 类操作系统安全；下篇第 9～14 章介绍 UNIX 类操作系统安全。读者可以根据自己的需要，选择阅读相关的章节。

第 1 章主要概述 Windows 系统安全要素。从系统安全模型的构成到安全账号的管理，从文件系统的使用到服务的控制管理，同时还探讨注册表、进程及驱动程序对系统安全性的影响。

第 2 章介绍账户安全管理。分别介绍系统管理员口令设置和账户安全管理、用户账户的管理、用户组的管理、账户策略及密码的安全，同时还介绍用户权限的安全和对域控制器的管理。

第 3 章讨论对系统资源的安全保护。主要包括对文件系统和共享资源的安全设置；应用程序和用户主目录的安全管理；注册表的安全管理；审核策略和系统策略文件；用户磁盘空间的限制和数据备份。

第 4 章介绍 IIS 的安全性管理。主要内容包括：IIS 的安全机制与安全设置，服务器安全整体解决方案及相关的安全措施，如内容分级设置、安全与权限设置、安全认证及 IP 地址及域名限制等。

第 5 章主要介绍证书服务与 SSL 安全协议。本章首先介绍安装配置证书服务和实现 SSL 证书颁发，然后介绍建立 SSL 安全站点和如何实现 Web 和 Internet 安全，最后给出 SSL 的安全漏洞及其解决方案。

第 6 章讲述 Windows 系统的安全漏洞与防范措施。分别讨论 Windows NT 漏洞与防范、Windows 2000 系统的安全漏洞与防范及 Windows XP 漏洞与防范。

第 7 章介绍 Windows 系统安全管理技巧。内容包括：用控制台配置安全系统和优化网络配置——TCP/IP 安全策略。

第 8 章介绍常用的安全工具，如扫描工具、网络数据流检测工具和加密工具等。

第 9 章讨论 UNIX 类操作系统的安全体系结构。内容包括物理的安全性、系统的安全性、用户的安全性、应用程序的安全性、数据库的安全性和安全管理原则及实现。

第 10 章主要介绍 UNIX 类操作系统下的用户安全策略，内容包括保护用户口令策略、root 账户的安全策略、用户访问控制策略和用户组的管理策略。

第 11 章重点讨论 UNIX 类操作系统下文件系统安全。从分区的安全策略到文件系统的安全加载、从文件的完整性检查到文件系统的数据备份都做了全面细致的分析。

第 12 章是 Web 服务器安全，内容有 Web 服务器的安全隐患及策略、Apache Web 服务的安全配置及安全 Web 协议 SSL 的介绍。

第 13 章讲述安全服务认证和网络加密协议。主要内容是 UUCP 系统及安全、Kerberos、Telnet 及 SSH 安全。

第 14 章介绍 UNIX 系统安全管理技巧。内容有系统安全设置技巧、日志和审计工具的使用，同时对 UNIX 类操作系统常见安全问题（FAQ）给予了解答。

本书的读者对象

本书适合以下读者对象：

- 信息安全专业本科高年级学生；
- 计算机、通信及相关专业的本科生和硕士生；
- 网站设计开发和维护的程序员、分析员和项目管理人员；
- 需要建立、实现和管理因特网和企业内部网的网络管理人员；
- 关注网络操作系统安全的技术人员；
- 关注网络安全的非专业人员和网络爱好者。

编　者

2005 年 10 月

目　　录

上　篇　Windows 类操作系统安全

下　篇　UNIX 类操作系统安全

上　篇

Windows 类操作系统安全

第 1 章　Windows 系统安全要素

1.1　Windows 系统安全模型

Windows 系统具有模块化的设计结构。所谓“模块”，就是一组被称做执行程序服务（Executive Service）的软件。这些“模块”运行在内核模式（Kernel Mode）下，内核模式之上是用户模式，由非特权服务组成，称为保护子系统（Protected Subsystem），其启动与否由用户决定。

必需的内核模式组件可组成自成系统的操作系统，并使用户模式组件利用它的服务运行在核心上，该结构称做微内核（Microkernel）结构。

Windows 系统的安全性根植于 Windows 系统的核心（Kernel）层，它为各层次提供一致的安全模型。Windows 系统安全模型是 Windows 系统中密不可分的子系统，控制着 Windows 系统中对象的访问（如文件、内存、打印机等）。在 Windows 系统中，对象实质上是指一系列信息集合体，封装了数据及处理过程，使之成为一个可被广泛引用的整体。当对象用于网络环境时，称之为资源；当对象在网络中共享时，称之为共享资源。

1.1.1　Windows 系统安全模型构成

Windows 的安全系统提供了对事件的审核及详细的跟踪手段来监控网络上资源的访问和应用。

Windows 系统安全模型由登录流程（Logon Process，LP）、本地安全权威（Local Security Authority，LSA）、安全账号管理器（Security Account Manager，SAM）和安全引用监视器（Security Reference Monitor，SRM）组合而成。

1.1.2　登录流程

登录流程接受本地用户的本地登录请求或者远程用户的远程登录请求，使用户和系统之间建立联系。如图 1-1 所示。

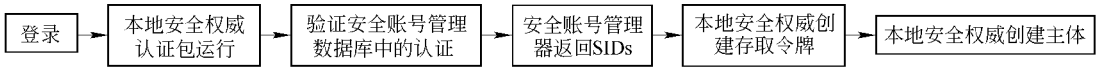

图 1-1　Windows 系统登录流程

登录开始，Windows 系统的 Winlogon 进程会显示一个安全性交互对话框，要求用户输入用户名、口令和用户希望登录的服务器/域。如果用户信息有效，系统将开始确认用户身份。Windows 系统把用户信息通过安全系统传输到安全账号管理器，并对用户身份进行确

认。安全账号管理器把用户的登录信息与服务器里的安全账号管理数据库进行比较，如果两者匹配，服务器将通知工作站允许用户进行访问。Winlogon 进程将调用 Win32 子系统为用户产生一个新的进程，同时服务器还将记录用户的一些信息，如用户享用的特权、主目录所在位置及工作站参数等。

然后本地安全权威开始构造访问令牌（Access Token），与用户进行的所有操作相连接，用户进行的操作与访问令牌一起构成一个主体（Subject）。当用户要求访问一个对象时，主体的访问令牌的内容将与对象的存取控制列表通过一个有效性访问程序进行比较，这个程序将决定允许或拒绝用户所发出的访问要求。

1.1.3 本地安全权威

本地安全权威是 Windows 系统的核心，它通过确认安全账号管理器中的数据信息来处理用户从本地或远程的登录。

本地安全权威确保用户有存取系统的权限，从而产生访问令牌，管理本地安全策略并提供交互式的用户认证服务。本地安全权威同时还控制审计方案和将安全引用监视器产生的审计信息记入日志。

本地安全权威具体担任以下职能：

- 在登录过程中建立访问令牌，提供用户有效身份证明；
- 使 Windows 系统能和第三方供应商的有效性确认软件包共同管理安全性策略；
- 控制审计策略；
- 确认用户对本系统的访问权限；
- 记录安全引用监视器生成的审计信息。

1.1.4 安全账号管理器

安全账号管理器维护账号的安全性管理数据库，即 SAM 数据库，又称目录数据库（Directory Database）。该数据库包含所有用户和组的账号信息，其中包含安全标识（Security Identifier，SID）。安全标识在账号新建时被创建，直到账号被删除。一旦用户账号被删除，就不能被重建，因为原先的账号不再存在了。用相同的名字新建的账号将被赋予不同的安全标识，不会保留原有的权限。

安全账号管理器提供本地安全权威使用的用户有效身份服务，使用安全账号管理器数据库来审计用户登录时输入的信息，并给用户返回一个安全标识及用户所属组的安全标识。当用户登录入网时，本地安全权威将创建一个访问令牌，该访问令牌包含用户名、用户所属的组及安全标识等信息，用户所有的程序将拥有访问令牌的拷贝。当用户要求访问一个对象时，系统将把访问令牌中的安全标识与对象的访问控制列表（Access Control List，ACL）进行对比，以确认用户是否具有对对象的访问权限。

根据网络的配置，在一个或多个 Windows 系统中可能存在不同的安全账号管理数据库。在登录时存取的安全账号管理数据库取决于用户是以工作站上的用户账号登录，还是以网络账号登录。

当一个用户在每一台工作站上都有独立账号时，登录时存取的安全账号管理数据库就位于用户登录的工作站上。

在一个有集中存放的用户账号的网络设置（如单域模式）中，在域控制器上有一个集中的安全账号管理数据库。如果以工作站上的账号登录，存取在工作站上的安全账号管理数据库；如果以域上的账号登录，则存取在域控制器上的安全账号管理数据库。

在另一种有集中存放用户账号的网络设置（如主控域的网络设置）中，在主域控制器（Master Domain Controller）上有一个被同时复制到该域的所有备份域控制器（Backup Domain Controller）上的安全账号管理数据库。如果以工作站上的用户账号登录，访问工作站上的安全账号管理数据库；如果以域上的用户账号登录，那么访问在主域控制器或备份域控制器上的安全账号管理数据库。备份域控制器分担主域控制器上用户请求的有效性确认工作。

被设置为单列服务器（Stand Alone Server）的 Windows 系统不做用户在域内的身份验证工作。

1.1.5　安全引用监视器

安全引用监视器是 Windows 系统的一个组成部分，它以内核模式（Kernel Mode）运行，负责检查 Windows 系统的存取合法性，以保护资源，使其免受非法存取和修改。安全引用监视器为对象的有效访问提供服务并为用户提供访问权限，同时还能够阻止非授权用户访问对象。为了确保所有类型对象都得到保护，安全引用监视器在系统中只维护一个有效性的复制访问代码。用户在要求访问对象时，必须通过安全引用监视器的有效验证，而不能直接访问对象。

另外，安全引用监视器还负责实施审计生成策略（由本地安全权威管理），它在验证对对象的存取的合法性和检查主体（用户账号）权限的同时，生成必要的审计信息。

安全引用监视器在系统中保留唯一的一份有效性的复制访问代码，这就保证了在整个Windows系统中对不同类型的对象提供一致的保护。

Windows 系统避免用户直接访问对象，用户向对象发出的访问请求必须首先由安全引用监视器进行合法性检查。例如，当用户打开一个文件进行编辑时，Windows 系统首先将该文件的安全描述符（Security Descriptor）与存储在访问令牌中的安全信息做比较，然后做出是否允许用户编辑该文件的决定。文件的安全描述符包括组成该文件的所有访问控制列表（Access Control Lists，ACLs）的所有访问控制项（Access Control Entries，ACEs）。一个没有访问控制列表的文件允许任何用户的任何类型的访问；一旦文件有访问控制列表，安全引用监视器必须检查访问控制列表中的每一个访问控制项，并决定用户是否能对该文件进行所需的特定访问。一旦安全引用监视器授权访问这个文件，就没有必要再对该文件的访问进行访问合法性检查，进一步对该文件的访问通过代表该文件的句柄进行。

安全引用监视器对用户是透明的，它是系统维护合法性检验的唯一组件，并能保护所有的对象。安全引用监视器还产生由本地安全权威记载的日志信息。