21 世纪网络工程师设计宝典丛书 6

Attack Signatures Glossary

网络核心技术内幕

网络攻击秘笈

本书配套光盘内容包括：
与本书配套的电子书

21 世纪网络工程师设计宝典丛书编委会　编

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

21 BEIJING HOPE

世纪网络工程师设计宝典丛书 6

Attack Signatures Glossary

网络核心技术内幕

网络攻击秘笈

本书配套光盘内容包括：
与本书配套的电子书

21世纪网络工程师设计宝典丛书编委会　编

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

本书是21世纪网络工程师设计宝典系列之一，是专为从事网络开发和应用的人而编写的。

随着 Internet 的飞速发展，尤其是近年来电子商务的快速发展，网络越来越与我们日常生活密不可分。但是，通过网络犯罪而对国家安全、企业安全和个人安全造成的损失日益严重。网络安全性已越来越成为人们关心的问题。

本书汇集了当前 400 余种典型的网络攻击手段，对各种攻击手段及其对被攻击方产生的影响进行了分析和介绍，并提供了相应的防范措施、对策以及解决方案。本书为网络安全工作者提供了全面而权威的安全指南，对创建和维护网站有着十分重要的意义。

本书条理清晰，内容丰富，技术新，实用性强。本书是企业 IT 人员、网络管理与维护人员的宝贵参考资料，是网站管理与维护的重要参考手册，同时也是高等院校相关专业师生自学、教学参考用书和社会相关领域培训班教材。

本书配套光盘内容包括：与本书配套电子书。

系　列　书：21世纪网络工程师设计宝典系列（6）
书　　名：网络核心技术内幕——网络攻击秘笈
文本著作者：21世纪网络工程师设计宝典丛书编写委员会
责任编辑：龙启铭
CD 制 作 者：希望多媒体创作中心
CD 测 试 者：希望多媒体测试部
出版、发行者：北京希望电子出版社
地　　址：北京海淀路82号，100080
网址：www.bhp.com.cn　E-mail：lwm@hope.com.cn
电话：010-62562329,62541992,62637101,62637102（图书发行,技术支持）
010-62633308,62633309（多媒体发行，技术支持）
010-62613322-215（门市）　010-62531267（编辑部）
经　　销：各地新华书店、软件连锁店
排　　版：希望图书输出中心
CD生产者：文录激光科技有限公司
文本印刷者：北京双青印刷厂
开本 / 规格：787×1092 毫米　16 开本　19.5 印张　446 千字
版次 / 印次：2000 年 4 月第 1 版　2000 年 4 月第 1 印刷
印　　数：0001~5000 册
本 版 号：ISBN7-900031-76-6/TP•76
定　　价：50.00 元（1CD，含配套书）

21世纪计算机网络工程师设计宝典丛书

编 委 会 名 单

序

21 世纪是网络经济时代，网络与我们同呼吸，网络大潮波涛滚滚、汹涌澎湃，社会生活节奏加快，世界是在知识和经济实力的较量中不断发展，前进的步伐大大加快。据我国有关部门统计，21 世纪我国最缺的人才领域之一是计算机网络工程人员和计算机网络管理人员。为满足社会对计算机网络人才日益高涨的需求，我们特与美国 Cisco 公司、美国耶鲁大学的部分计算机和通信专家共同策划和开发了、为培养 21 世纪网络工程专业人才用的又一套热门书："21 世纪网络工程师宝典丛书"，共计 14 种，书名如下：

1.《网络核心技术内幕—专业 IP 网络规划与设计》

2.《网络核心技术内幕—Cisco 网络安全解决方案》

3.《网络核心技术内幕—组网技术解决方案》

4.《网络核心技术内幕—Cisco Debug 命令参考》

5.《网络核心技术内幕—网络设计教程》

6.《网络核心技术内幕—网络攻击秘笈》

7.《网络核心技术内幕—Cisco Works 使用手册》

8.《网络核心技术内幕—Cisco IP/TV 开发指南》

9.《网络核心技术内幕—Cisco PIX 防火墙配置指南》

10.《网络核心技术内幕—S/390 专用配置指南》

11.《网络核心技术内幕—Cisco IOS 新功能详解》

12.《网络核心技术内幕—网络协议解决方案》

13.《网络核心技术内幕—网络电话开发指南》

14.《网络核心技术内幕—综合 IP 网络设计解决方案》

每种书由以下主要内容构成。

1.**《网络核心技术内幕—专业 IP 网络规划与设计》**：是美国 Cisco 公司全球网络专家资格认证书的权威培训教材。全书由四部分、九章和五个附录组成。第一部分介绍网络稳定性的基础——网络的分层，讨论了分层规划的原则、地址分配和聚和、各层的冗余和网络规划原则的应用。第二部分介绍了各种先进的内部网关协议，包括 OSPF，IS-IS，EIGRP 网络规划。第三部分介绍网络的扩展，讨论了 BGP 核心层和网络的可扩展性以及其它大规模核心层。第四部分作为本书的附录介绍了 OSPF，IS-IS，EIGRP，BGP 的基础。在介绍基础理论的同时，本书各章后都附有实例学习和复习题，并针对部分疑难问题提出相应的解决方案，附录 E 中有各章复习题的答案。

本书结构清晰，内容丰富，技术新、实用性强，不但是想获取 Cisco 网络专家资格认证的广大科技人员必读的教科书，同时也是从事网络应用设计和开发的广大工程人员、开发人员、网络管理人员的重要参考书，高等院校相关专业师生重要的自学、教学参考用书和社会相关领域培训班教材。

本书配套光盘内容包括：1. 与本书配套电子书；2. 送"计算机基础知识全面速成"多媒体学习软件。

2.**《网络核心技术内幕—网络安全解决方案》**：本书全面介绍了如何针对 Cisco 网络设备配置 Cisco IOS 安全特性。通过 Cisco IOS 安全特性的配置，使我们的网络能够避免有意和无意的攻击，避免由于合法用户的误操作造成的数据丢失或泄露，从而保护网络系统的安全。全书共分六部分：认证、授权及记帐（AAA）、安全服务器协议、流量过滤和防火墙、IP 安全和加密技术、其它安全特性和附录。认证提供了识别用户的方法，它在允许用户访问网络以及网络资源之前确认用户的身份；授权提供了远程访问控制的方法，它包括一次性授权和对每个服务进行授权；记帐提供了收集和发送帐单信息、审计信息以及报告信息的手段。

安全服务器协议部分介绍了配置 RADIUS、Kerberos、TACACS+、TACACS 和扩展 TACACS 的方法、命令和过程。流量过滤和防火墙部分介绍了如何配置网络设备进行流量过滤以及如何把网络设备配置成精细入微的防火墙。IP 安全与加密部分介绍配置 Cisco 加密技术、配置 IPSec、配置证书认证机构（CA）的互操作能力以及配置 Internet 密钥交换的方法。其它安全特性部分介绍了进一步加强网络安全的其它技术与措施。

3.**《网络核心技术内幕—组网技术解决方案》**：随着网络应用的不断深入，企业组网已经成为发展的必然趋势，如何设计企业组网的整套软、硬件解决方案已经成为许多 IT 人员密切关心的问题。本书提供了一套 Cisco 系统公司组网技术切实可行的解决方案。

全书由五部分，15 章构成。第一部分介绍了如何用隧道技术访问 VPN 方案；第二部分介绍了 Cisco 安全 VPN 客户方案指南，讨论了虚拟专用网、Cisco 路由器的相互操作性以及使用预共享密钥、使用数字证书和使用 Internet 密钥交换方式配置的业务案例；第三部分用 37 个例子介绍了侵入探测计划指南；第四部分介绍了如何使用 CiscoSecure 与 Oracle 的分布式数据库特性；第五部分介绍了 Cisco SS7/CCS7 拨号访问方案系统集成指南。

本书结构清晰，事例丰富，技术新，实用性强。本书是企业 IT 人员、专业网络公司技术人员和系统集成人员的宝贵资料，是解决组网方案的重要参考手册，也是大、中专院校介绍网络技术重要的教学、自学参考用书和社会相关领域培训班教材。

4.**《网络核心技术内幕—Cisco Debug 命令参考》**：随着网络应用的不断深入，企业组网已经成为发展的必然趋势。如何设计企业组网的整套软、硬件解决方案已成为许多 IT 人员密切关心的问题。当网络出现故障时，尽快解决问题尤为关键。通过使用 Debug 命令，就可以快速地查找出故障发生的原因和地方，为故障的解决提供依据。

本书详细介绍了 Debug 命令的使用方法，以及命令的使用对路由器将产生的影响。对每种方法都给出了其命令格式、语法说明、使用说明等，并给出了命令的输出实例。用典型范例教读者如何尽快学习和掌握 Cisco Debug 命令的使用是本书最大的特色。

5.**《网络核心技术内幕—网络设计教程》**：本书通过以网络设计概念、网络设计基本分析、设计要点、实际案例设计、巩固思考题的组成形式，使读者能够达到学习和掌握网络设计的效果，同时涵盖了全球著名网络设计师认证考试 CCDA 的所有课题。全书共分为七大部分。第一部分介绍了现代网络技术的发展和基本概念；第二部分提供了中小规模的商务解决方案框架；第三部分介绍了怎样准确地描述现有的网络，怎样确定客户的网络需求；第四部分详细介绍在特定的拓朴结构和互联网络约束条件下，如何设计网络来满足客户对性能、安全、容量和可伸缩性的需求；第五部分描述如何建立和测试网络原型或先导；第六部分提供了一个 CCDA 考试样题；第七部分是一些附录，在附录里提供了大量有用的附加信息，其中包括有四个案例分析，还有各章中问题的参考答案。最后给出了一个英汉对照的术语表。

6.**《网络核心技术内幕—网络攻击秘笈》**：随着 Internet 的飞速发展，尤其是近年来电子商务的快速发展，网络越来越与我们日常生活密不可分。但是，通过网络犯罪而对国家安全、企业安全和个人安全造成的损失日益严重。网络安全性已成为最为关心和棘手的问题。

本书汇聚了当今 400 余种典型网络攻击方法和手段，并对每种攻击手段和方法进行了全面的技术分析并提出了相应的解决措施，为从事网络安全开发和应用的广大科技人员提供了全面而权威的网络安全指南，对创建和维护网站有着十分重要的意义。

7.**《网络核心技术内幕—CiscoWorks 使用手册》**：本书详细地介绍 CiscoWorks 4.0 软件在多种软件平台下的运行和操作方法，全面地介绍利用 CiscoWorks 对 Cisco 网络设备的管理、状态监控和故障诊断技术，并系统地阐述网络安全和用户的管理方法。全书共分八章，主要内容包括：CiscoWorks 的功能和性能以及在多种平台下的应用程序； 利用 CiscoWorks 软件建立网络设备信息库并对其进行管理的方法； 利用

CiscoWorks 软件对网络设备和网络系统进行故障诊断的策略与技术和应用程序的操作方法；利用 CiscoWorks 软件对网络系统进行管理的方法，以便提高系统的运行效率和管理水平；利用 CiscoWorks 软件对 Cisco 网络设备进行配置的方法； CiscoWorks 软件对网络安全和用户帐户的管理方法； CiscoWorks 软件对网络及其设备维护信息库的管理技术和 CiscoWorks 软件如何对自身应用程序的管理与调度的方法。

本书图文并茂，内容丰富，技术新颖，实用性强。

8.**《网络核心技术内幕—IP/TV 开发指南》**：本书是专为从事网络开发和网络应用人员编写的。随着网络应用的不断深入，企业组网已经成为发展的必然趋势。而多媒体在网络上的应用更成为网络发展的一种时尚。Cisco 迎合这种发展的潮流，通过 IP / TV 使人们的梦想成为可能。

IP/TV 是一个客户/服务器体系结构的软件系统，为基于 IP 协议的局域网或广域网上的广大用户提供实时节目转播或预定节目数字视频和音频流的播放。

全书共分三部分：分别介绍 IP/TV 内容管理器，IP/TV 服务器，IP/TV Viewer。其中内容管理器部分主要介绍系统管理员或者广播管理员如何利用 IP/TV Content Manager 来建立和管理 IP/TV 实时节目转播或预定节目、频道、记录和在 IP/TV Server 之间的文件传输。IP/TV Server 则介绍了如何进行对内容管理器的控制，包括多点广播、单点传输点播节目、记录预定的节目，以及如何根据在内容管理器中定义的节目单点传输节目。而用户则需要通过 IP/TV Viewer 观看节目。IP/TV Viewer 从内容管理器取得节目信息，显示 IP/TV 服务器广播或单独播放的节目。也可以通过国际广播主干（Mbone）或从别的服务器传送的与 Mbone 兼容的广播节目获取所需的节目。

IP/TV 将一个完全动感的视频空间展现给终端用户，无需专用的视频电缆、显示器和会议室，并提供了对使用 ActiveMovie 结构的最新视频流格式的支持。可用于桌面电视会议、视频点播、网上培训、远程教学、团体通讯、制造过程监控，以及监视系统等。其前卫的设计思想展现了网络发展之必然，具有广阔的发展前景。

9.**《网络核心技术内幕—Cisco PIX 防火墙配置指南》**：本书是一本介绍 Cisco PIX 防火墙配置的指导书。全书共由 7 章组成，主要内容包括引言，配置 PIX 防火墙，高级配置，配置 IPSec，配置实例，命令参考，PIX 515 配置。

本书根据实际工程项目操作所需知识编写而成，可操作性强，内容新颖、丰富、实用性很强。同时，本书还附有大量的实例。

10.**《网络核心技术内幕—S/390 专用配置指南》**：本书是专为从事网络开发和应用人员编写的。

Cisco IOS for S/390 是 Cisco 公司专门为 IBM 主机系列的 S/390 开发的专用通信系统。本书包括了 Cisco IOS 用户指南、S/390 机 Cisco 配置指南、S/390 机规划指南和 S/390 机的 Cisco IOS 系统管理指南四部分内容。每部分内容都详细描述了 Cisco 实现的协议和技术、相关的配置任务，并包含综合配置的示例。每个命令索引都补充其相应配置内容并提供了完整的命令语法信息。

11.**《网络核心技术内幕—Cisco 新功能详解》**：本书是专为从事网络开发和应用的人员编写的。主要介绍 Cisco IOS 的新功能，涵盖了 Cisco IOS 版本增强特征的方方面面，主要包括防火墙功能集、各种设备互通、配置的各种增强特征、三级 DES 加密、动态数据包传输接口处理、PPP 等。本书对 Cisco IOS 版本的新特征进行了详尽、全面、透彻的介绍。本书结构清晰，内容丰富，技术新，实用性强。

12.**《网络核心技术内幕—网络协议解决方案》**：本书由 16 章组成，主要介绍 AppleTalk、Novell IPX、Apollo Domain、Banyan VINES、DECnet、ISO CLNS 和 XNS 等路由协议的网络解决方案，Cisco 实现的协议和技术、相关的配置任务，并包含综合配置的示例。每个命令索引都补充其相应配置内容并提供了完整的命令语法信息。

13.**《网络核心技术内幕—网络电话开发指南》**：专为从事网络电话开发和应用的人员编写的，是一本介绍 Cisco 智能电话控制器的指导书。全书由 6 章和 3 个附录组成，主要内容包括：电话控制器软件概述、

准备电话控制器、电话控制器的操作、检索呼叫详细记录及网络测量、维护过程和系统故障诊断与调试。附录分别介绍了配置数据文件参考、MML 命令和 UNIX 系统操作及安装。

本书内容新颖、结构清晰、丰富、实用性强，并附有大量的图例。书中既有对 Cisco 智能电话控制器软件的详细介绍，又有对其调试及安装的全面描述。

14.**《网络核心技术内幕—综合 IP 网络设计解决方案》**：IP 网络是现代网络技术的一个重要发展方向。建设综合 IP 网络对提高现代企业的竞争力尤为关键。本书对建设综合 IP 网络进行了全面阐述。本书分为两大部分：Internet 概述、网络核心与分布，内容涉及网络设计的概述，WAN、LAN 和路由器技术，以及路由协议的配置，QoS 发布和网络管理。第一部分包括 5 章：数据网络的发展、IP 基础、网络技术、网络拓扑结构设计、路由器等。第二部分包括 11 章：路由选择信息协议、路由选择信息协议版本 2、增强内部网关选择协议、开放最短路径优先、中间系统到中间系统、边界网关协议、迁移技术、协议无关多播、服务特性的质量、网络操作和管理、设计和配置的案例研究等。

本丛书具有以下特点：

1. **技术新，具有前瞻性** 紧跟 90 年代末、21 世纪初国际网络最新技术的发展是本丛书第一大特色。套书中介绍的网络规划与建设、软件和硬件的配置、安全与维护技术、网络电话的开发等技术均是国际目前最具代表、最流行的网络产品和技术。

2. **技术全面、内容丰富** 本丛书从网络巨头 Cisco 公司全球网络工程师资格认证考试 CCDA 教材、网络安全解决方案、组网技术解决方案、网络配置、如何阻挡和对抗黑客的攻击、网络协议解决方案到网络电话的开发、典型网络应用范例 S/390 专用配置，高起点、高定位，技术新、全面、系统、内容丰富和与当前市场网络产品同步或超前则是本丛书第二大特色。

3. **范例经典，实用性强** 本丛书结构设计合理、概念清晰、范例经典、可操作性和实用性强，所针对的问题具有现实性和代表性，解决方法具有实际指导性是本丛书第三大特色。

通过书中范例的学习，读者在学习和工作中可达到事半功倍的目的。本丛书不但是从事网络开发、应用和管理的广大网络技术人员的指导性读物，而且也是高等院校相关专业师生自学、教学用书和社会相关领域培训班的教材。

在此特别感谢世界通信巨头 Cisco 公司的首席技术顾问、美国 ATD 国家实验室主任、耶鲁大学教授约瑟夫·帕利洛先生，本丛书就是在他的大力帮助和协调下才得以完成。感谢美国国家网络安全委员会成员、麻省理工学院教授琼斯·雷蒙女士，耶鲁大学教授米勒·汉克斯先生，Cisco 公司技术主任蒂姆·克拉克博士，由于他们的全力参与和辛勤劳动，本丛书能够及时完稿和及时面市。

特别要感谢的是本丛书的翻译人员：刘大伟、曾春平、刘道云、李志、程永敬、邱仲潘、杜德宁、夏红山、杨键、韩平；编辑人员：刘晓融、龙启铭、马宏华、王玉玲、周艳、周凤明、苏静、郭淑珍、赵玉芳、徐建华； 录排人员：全卫、杜海燕、李毅、刘桂英、董淑红、马君、周宇、邓娇龙；美工设计人员张洁、徐立平； 光盘制作人员尹飒爽等，是他们的加班、加点、忘我的工作，才使本丛书如期付印出版，在此表示深切的谢意！

尽管我们很努力，但相信书中会有不少需要修改之处，希望能得到各界读者的信息反馈，以期为大家提供更好的作品。

北京希望电子出版社

2000 年 3 月

目 录

攻击类型

拒绝服务攻击

一般情况下，拒绝服务攻击（Denial of Service Attacks）通过使关键系统资源过载，从而使受害工作站停止部分或全部服务。拒绝服务攻击的示例包括 SYN Flood，Ping Flood 和 Windows Out Of Band（WinNuke）等类型的攻击。

- Apache Web Server Denial of Service Attack
- Ascend Kill
- Chargen
- Cisco CR
- E-mail Qmail Length
- E-mail Qmail Rcpt
- Echo
- Finger Bomb
- HTTP IISExAir DoS
- Land Denial of Service Attack
- Land UDP
- Ping Flooding
- Ping Of Death
- Rwhod
- SMURF Denial of Service Attack
- SNMP Delete WINS Database Attack
- SYN Flood
- Talk Flash
- TearDrop Fragmentation Attack
- UDP Bomb
- Win IGMP
- Windows Out of Band (OOB)

非授权访问尝试

非授权访问尝试（Unauthorized Access Attempts）是攻击者对被保护文件进行读、写或执行的尝试，也包括为获得被保护访问权限所做的尝试。非授权访问尝试的示例包括 FTP root 和 e-mail WIZ 等。

- Back Orifice Default Install Check
- Back Orifice 2000 Install Check
- DNS Hostname Overflow

- DNS Length Overflow
- E-mail DEBUG
- E-mail Decode
- E-mail Ehlo
- E-mail Listserv
- E-mail Pipe
- E-mail VRFY Overflow
- E-mail WIZ
- EvilFTP Backdoor
- FSP Detected
- FTP arg Core Dump
- FTP Bounce Attack
- FTP CWD ~root
- FTP Privileged Bounce Attack
- FTP Privileged Port Attack
- FTP Site Exec..
- FTP Site Exec Tar
- Generic Intel Overflow
- HP/UX RemoteWatch
- HP OpenView SNMP Backdoor
- HTTP ..
- HTTP AnyForm
- HTTP AnyFormPost
- HTTP Cachemgr
- HTTP campas cgi-bin
- HTTP Carbo Server
- HTTP Classifieds Post
- HTTP Cold Fusion
- HTTP Glimpse cgi-bin
- HTTP HTMLScript
- HTTP IE BAT
- HTTP IIS 3.0 Asp 2E
- HTTP IIS 3.0 Asp Dot
- HTTP IISHTR Overflow
- HTTP Info2WWW
- HTTP Internet Explorer 3.0 .URL/.LNK
- HTTP JJ
- HTTP MachineInfo
- HTTP NCSA Buffer Overflow
- HTTP Novell Convert
- HTTP Novell Files
- HTTP NT8.3 Filename
- HTTP Pfdisplay Execute
- HTTP Pfdisplay Read

- HTTP PHF
- HTTP PHP Buffer Overflow
- HTTP PHP File Read
- HTTP RegEcho
- HTTP RobotsTxt
- HTTP RpcNLog
- HTTP SCO View-Source
- HTTP SGI Handler
- HTTP SGI WebDist
- HTTP SiteCsc Access
- HTTP UNIX Passwords
- HTTP Verity Search
- HTTP Webgais
- HTTP Websendmail
- HTTP Website Uploader
- HTTP Website Win-C-Sample
- HTTP WWW-Count cgi-bin
- Ident Buffer Overflow
- Ident Newline
- IMAP Buffer Overflow
- INN Buffer Overflow
- INN Control Message
- IP Fragmentation
- IRCD Buffer Overflow
- Kerberos IV User Snarf
- NetBus
- NetBus Pro
- NFS Guess Check
- NFS Mknod Check
- NFS UID Check
- NISd Buffer Overflow Attack
- PCNFSD Exec
- Perl Fingerd Check
- POP Buffer Overflow
- Rlogin -froot
- RPC.Admind Check
- RPC Cmsd Overflow
- RTM Finger
- SAMBA SMB Password Overrun
- Statd Buffer Overflow Attack
- Statd File Creation Check
- SubSeven Scan
- Sun SNMP Backdoor
- TCP Hijacking Tools Decode

- TFTP Get
- TFTP Put
- ToolTalk Overflow
- Windows Password Cache File Access
- Ypupdated Exec Check

预攻击探测

在连续的非授权访问尝试过程中，攻击者为了获得网络内部的信息及网络周围的信息，诸如用户名称和口令等，通常使用这种攻击尝试。预攻击探测的示例包括 SATAN 扫描、端口扫描和 IP 半途扫描等。

- Cisco Ident
- Cybercop Scanner
- DNS All
- DNS HInfo Request Decode
- DNS Zone Transfers
- DNS Zone Transfers from High Ports
- E-mail EXPN
- E-mail EXPN Overflow
- E-mail Helo Overflow
- E-mail VRFY
- FTP SYST Command Decode
- HTTP Netscape PageServices
- HTTP Netscape SpaceView
- HTTP nph-test-cgi
- HTTP SGI Wrap
- HTTP ShellHistory
- HTTP test-cgi
- IP Half Scan
- ISS Scan Check
- Nmap Scan
- Portmapper Program Dump Decode
- Portscan Detection
- Queso Scan
- SATAN
- Trace Route Decode
- UDP Port Scan

可疑活动

通常所定义的“标准”网络通信范畴之外的通信模式，它也可指网络上不希望有的