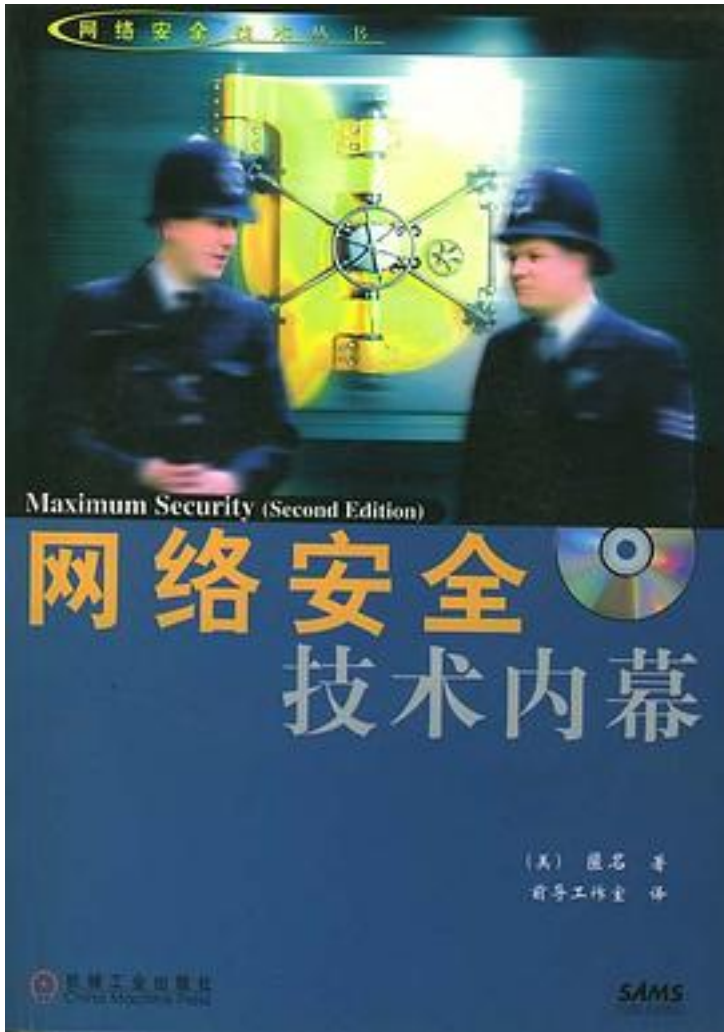


网络安全技术内幕



[网络安全技术内幕_下载链接1](#)

著者:(美)匿名

出版者:机械工业出版社

出版时间:1999-04

装帧:平装

isbn:9787111071822

这是一本介绍网络安全的书，从组织结构上说，分为三部分：技术发展、工具软件和参

考文献。技术发展部分介绍了安全方面的背景知识，包括Internet的结构、Internet上运行的协议（主要是介绍TCP/IP协议）、一名黑客所具有的知识以及安全的一些概念，如加密算法与标准译码以及信息、截取等。工具软件部分详细讲述一些黑客常用的攻击方法，如破坏性装置（邮件炸弹、病毒等）、Internet端口与服务扫描程序、口令攻击程序、特洛伊木马、嗅探器等，并给出了很多黑客常用的攻击工具。在阐述攻击工具之后，作者也对防止攻击提出了很多很好的解决方案，如防火墙、登录与审计工具、各种加密方法等。参考文献部分主要是针对那些要进一步深入研究安全的读者，作者将Internet和各种杂志上的很多有关安全的文章列举出来、以供读者参考。

本书适用于Internet网友和对网络与系统平台的安全有一定要求的信息主管，同时对于国内安全保密研究方面的专家，也具有非常不错的参考价值。

作者介绍:

目录: 目 录

译者序

前言

第一部分 开始阶段

第1章 我为什么要写这本书

1.1 安全需要的现实性

1.2问题之源

1.2.1目标主机的错误配置

1.2.2系统缺陷或开发商缺乏反应

1.2.3为什么安全培训是重要的

1.3法人方面

1.4政府

1.5孤独的远程网络冲浪

1.6小结

第2章 如何使用本书

2.1怎样用本书

2.2几种工具的下载地址

2.2.1FTP客户程序

2.2.2压缩文件格式

2.2.3文本文件格式

2.3编程语言

2.4本书使用方法

2.4.1学习Internet安全的基本知识

2.4.2利用本书保护网络安全

2.4.3利用本书作安全研究

2.5本书的局限性

2.5.1时效性

2.5.2功用性

2.6本书结构

2.7本书的零碎问题

2.8小结

第二部分 理解领域范围

第3章 网络的产生: Internet

3.1产生 (1962~1969)

3.2UNIX的产生 (1969~1973)

3.3C语言

3.3.1Internet的形成期 (1972~1975)

3.3.2进入UNIX时代

3.3.3UNIX和Internet的共同发展

3.3.4UNIX的基本特征

3.3.5XWindows系统

3.3.6UNIX上运行的应用程序

3.3.7UNIX与Internet安全的关系

3.4继续：现代Internet

3.4.1Internet服务提供者

3.4.2将来

3.5小结

第4章 TCP/IP简介

4.1什么是TCP/IP

4.1.1TCP/IP协议包中的协议类型

4.1.2 TCP/IP历史

4.1.3哪些平台支持TCP/IP

4.2TCP/IP的工作

4.3协议

4.4TCP/IP就是Internet

4.5小结

第5章 黑客和破译者

5.1黑客和破译者之间的区别

5.1.1MensRea

5.1.2计算机语言

5.1.3RandalSchwartz

5.2所有这些从何处开始

5.3今日状况：网络战争

5.3.1黑客举例

5.3.2破译者举例

5.4小结

第6章 黑客攻击的对象

6.1术语“被破译”的意思

6.2政府

6.2.1国防信息系统网络

6.2.2美国的海军和NASA

6.2.3对五角大楼的攻击

6.2.4政府安全

6.2.5总统关键设施保护委员会

6.2.6国家设施保护中心

6.2.7对政府工作漏洞的总结

6.3公共站点

6.3.1StarWave事件

6.3.2其他信用卡案例

6.3.3趋势

6.3.4Farmer的安全综述：

DustingMoscow

6.3.5Ernst&YoungLLP/Information

Week的信息安全综述

6.4警告

6.5小结

第7章Internet战争

7.1Internet可以改变你的生活

7.2我们不能很好相处吗

7.3朋友或敌人

7.4Internet可以用作间谍活动吗

7.5威胁将更个人化

- 7.5.1谁掌握了秘密
- 7.5.2美国能保护国家信息设备的安全吗
- 7.6信息攻击将会是什么样子
- 7.7Y2K
- 7.8不远的未来
- 7.9小结
- 7.10关于信息战的资源
- 7.11关于信息战的书
- 7.12关于Y2K的资源
- 7.13 Y2K的书
- 第8章 安全概念
- 8.1我们迫切需要Internet
- 8.2评估公司的特殊状况
- 8.3认证和承诺
- 8.3.1Cooper&LybrandL.L.P, Resource ProtectionServices
- 8.3.2TheAmericanInstituteofCertified PublicAccountants
- 8.3.3InternationalComputerSecurity Association
- 8.3.4 TroySystems
- 8.3.5做为保证而非责任的认证
- 8.4在哪儿接受训练
- 8.5一般训练
- 8.5.1LucentTechnologies, Inc
- 8.5.2GreatCircleAssociates, Inc
- 8.5.3LearningTreeInternational
- 8.5.4NSCSystemGroup, Inc
- 8.5.5TrainingOnVideo
- 8.6高级训练
- 8.7用Co-Location方法解决
- 8.8雇佣外面的安全顾问
- 8.8.1花费
- 8.8.2根本问题
- 8.8.3关于你的系统管理员
- 8.9顾问和其他解决方案
- 第三部分 工具
- 第9章 破坏性设备
- 9.1什么是破坏性设备
- 9.1.1破坏性设备对安全的威胁
- 9.1.2电子邮件炸弹
- 9.1.3电子邮件炸弹程序包
- 9.1.4电子邮件炸弹的处理
- 9.1.5电子邮件炸弹对安全的威胁
- 9.1.6列表链接
- 9.1.7邮件中继
- 9.1.8服务拒绝攻击
- 9.1.9你将会在哪里发现服务拒绝攻击
- 9.1.10服务拒绝目录
- 9.1.11著名的服务拒绝攻击
- 9.1.12对硬件的服务拒绝攻击
- 9.1.13其他的服务拒绝工具
- 9.1.14其他的服务拒绝资源

- 9.1.15病毒
- 9.1.16什么是计算机病毒
- 9.1.17谁编写病毒及其原因
- 9.1.18病毒是如何产生的
- 9.1.19病毒是用何种语言编写的
- 9.1.20病毒是如何工作的
- 9.1.21主引导区记录病毒
- 9.1.22反病毒工具
- 9.1.23相关文献及站点
- 9.2 小结
- 第10章 扫描程序
 - 10.1扫描程序怎样工作
 - 10.2哪些平台上有扫描程序
 - 10.3运行扫描程序的系统要求
 - 10.4创建扫描程序的难度
 - 10.5扫描程序合法吗
 - 10.6扫描程序对Internet安全的重要性
 - 10.7扫描程序对安全所造成的影响
 - 10.8扫描程序
 - 10.8.1Nessus
 - 10.8.2Nessus
 - 10.8.3Strobe
 - 10.8.4SATAN
 - 10.8.5Ballista
 - 10.8.6Jakal
 - 10.8.7IdentTCPscan
 - 10.8.8Ogre
 - 10.8.9WebTrendsSecurityScanner
 - 10.8.10InternetSecurityScanner和SAFEsuite
 - 10.8.11防护墙的另一侧
 - 10.8.12CONNECT
 - 10.8.13FSPScan
 - 10.8.14XSCAN
 - 10.9在其他平台上
 - 10.10小结
- 第11章 口令攻击程序
 - 11.1 口令攻击程序的概念
 - 11.1.1口令破译者如何工作
 - 11.1.2密码学
 - 11.1.3ROT-13
 - 11.1.4DES与Crypt
 - 11.2口令攻击程序的重要性
 - 11.3口令攻击程序
 - 11.4 用于WindowsNT的口令攻击程序
 - 11.4.10phtCrack2.0
 - 11.4.2MidwesternCommerce公司的ScanNT
 - 11.4.3Somarsoft的NTCrack
 - 11.4.4 MidwesternCommerce公司的PasswdNT
 - 11.5UNIX上的口令攻击程序
 - 11.5.1Crack
 - 11.5.2Jackal的CrackerJack

- 11.5.3PaceCrack95
- 11.5.4 CryptKeeper的Q巴『ack
- 11.5.5SolarDesigner的Johnthe Ripper
- 11.5.6Remote和Zabkar的Hade
- 11.5.7Sorcerer的StarCracker
- 11.5.8Racketeer和Presense的HellfireCracker
- 11.5.9Roche'sCrypt的XIT
- 11.5.10Grenadier的Claymore
- 11.5.11ChristianBeaumont的Guess
- 11.5.12ComputerIncidentAdvisory Capability (CIAC) DOE的Merlin
- 11.6其他类型的口令攻击程序
- 11.6.1MichaelA.Quinlan的ZipCrack
- 11.6.2FastZip2.0
- 11.6.3GabrielFineman的Decrypt
- 11.6.4Glide
- 11.6.5AMIDecode
- 11.6.6JamesO' Kane的NetCrack
- 11.6.7MarkMiller的PGPCrack
- 11.6.8RichardSpillman的ICSToolkit
- 11.6.9 E.Kuslich的EXCrack
- 11.6.10LyalCollins的CP.EXE
- 11.7资源
- 11.7.1关于UNIX口令安全
- 11.7.2其他资源和文档
- 11.8小结
- 第12章 特洛伊木马
- 12.1什么是特洛伊木马
- 12.2特洛伊是来自何处
- 12.3特洛伊出现在哪里
- 12.4特洛伊被真正发现的频度
- 12.5特洛伊表明什么层次的危险
- 12.6怎样检测特洛伊
- 12.6.1MD5
- 12.6.2Hobgoblin
- 12.6.3在其他平台上
- 12.7资源
- 12.8小结
- 第13章 嗅探器
- 13.1嗅探器的安全危害
- 13.1.1局域网与数据流量
- 13.1.2报文发送
- 13.2嗅探器能够造成的危害
- 13.3是不是真的有人发现过嗅探器的攻击
- 13.4嗅探器获取的信息
- 13.5嗅探器在何处出现
- 13.6从何处可以得到嗅探器
- 13.6.1商用嗅探器
- 13.6.2NetworkAssociates公司的ATM嗅探式网络分析器

- 13.6.3 Shomiti系统公司的CenturyLAN分析器
- 13.6.4 KlosTechnologies公司的PacketView
- 13.6.5 NetworkProbe8000
- 13.6.6 LANWatch
- 13.6.7 EtherPeek
- 13.6.8 NetMinderEthernet
- 13.6.9 IBM的DatagLANce网络分析器
- 13.6.10 LinkViewInternet监视器
- 13.6.11 ProConvert
- 13.6.12 LANdecoder32
- 13.6.13 NetxRayAnalyzer
- 13.6.14 NetAnt协议分析器
- 13.7 可免费获取的嗅探程序
- 13.7.1 ESniff
- 13.7.2 Gobbler
- 13.7.3 ETHLOAD
- 13.7.4 Netman
- 13.7.5 LinSniff
- 13.7.6 SunSniff
- 13.7.7 linuxsniffer.c
- 13.8 抵御嗅探器的攻击
- 13.9 检测和消灭嗅探器
- 13.9.1 安全的拓扑结构
- 13.9.2 会话加密
- 13.10 小结
- 13.11 关于嗅探器方面更多的资料
- 第14章 防火墙
- 14.1 防火墙简介
- 14.2 防火墙执行的其他任务
- 14.3 防火墙构件
- 14.4 防火墙的类型
- 14.4.1 网络级防火墙
- 14.4.2 应用代理防火墙（应用网关）
- 14.4.3 确信信息系统防火墙工具包
- 14.5 防火墙综述
- 14.6 创建防火墙的重要步骤
- 14.6.1 确定拓扑结构 应用和协议需求
- 14.6.2 分析本组织中的可信任关系
- 14.6.3 制定规则并选择合适的防火墙
- 14.6.4 使用及测试防火墙
- 14.6.5 防火墙的安全问题
- 14.6.6 CiscoPIXDES漏洞
- 14.6.7 Firewall-1保留关键字漏洞
- 14.7 商用防火墙
- 14.7.1 AltaVistaFirewal198
- 14.7.2 ANSInterLock
- 14.7.3 Avertis
- 14.7.4 BorderManager
- 14.7.5 Conclave
- 14.7.6 CSMPProxy/EnterpriseEdition
- 14.7.7 CyberGuard防火墙

- 14.7.8 CyberShield
- 14.7.9 Elron 防火墙/Secure
- 14.7.10 FirewallA3.0
- 14.7.11 GauntletInternet 防火墙
- 14.7.12 GNAT 防火墙盒
- 14.7.13 Guardian
- 14.7.14 IBM eNetwork 防火墙
- 14.7.15 Interceptor 防火墙工具
- 14.7.16 NETBuilder
- 14.7.17 NetRoadTrafficWARE 防火墙
- 14.7.18 NetScreenA0
- 14.7.19 PIX 防火墙4.1
- 14.7.20 Raptor 防火墙
- 14.7.21 SecureAccess
- 14.7.22 SecurIT 防火墙
- 14.7.23 SunScreen
- 14.8 小结
- 第15章 日志和审计工具
- 15.1 日志工具
- 15.2 使用更多日志工具的原因
- 15.3 网络监视和数据收集
- 15.3.1 SWATCH
- 15.3.2 Watcher
- 15.3.3 lsof
- 15.3.4 Websense
- 15.3.5 适用于防火墙和VPN的
WebTrends
- 15.3.6 Win—LogV1
- 15.3.7 MLOG
- 15.3.8 NOCOL/NetConsoleV4.0
- 15.3.9 PingLogger
- 15.4 分析日志文件的工具
- 15.4.1 NestWatch
- 15.4.2 NetTracker
- 15.4.3 LogSurfer
- 15.4.4 VBStatS
- 15.4.5 Netlog
- 15.4.6 Analog
- 15.5 特别日志工具
- 15.5.1 Courtney
- 15.5.2 Gabriel
- 15.6 小结
- 第四部分 平台和安全
- 第16章 漏洞
- 16.1 漏洞的概念
- 16.2 关于时间性
- 16.3 漏洞如何出现
- 16.4 开采数据
- 16.5 究竟需要多大的安全度
- 16.6 一般资源
- 16.6.1 计算机紧急事件反应小组
- 16.6.2 美国能源部计算机事件咨询库
- 16.6.3 国立标准和技术协会计算机
安全资源交换所

- 16.6.4美国国防部网络信息中心
- 16.6.5BUGTRAQ文档
- 16.6.6事件响应和安全小组论坛
- 16.6.7Windows95bug文档
- 16.7邮件列表
- 16.8usenet新闻组
- 16.9厂家安全邮件列表、补丁仓库以及资源
 - 16.9.1SiliconGraphics安全总部
 - 16.9.2Sun安全公告文档
 - 16.9.3ISSNT安全邮件列表
 - 16.9.4国立健康协会
 - 16.9.5计算机和网络安全参考目录
 - 16.9.6EugeneSpafford的安全活动表
- 16.10小结
- 第17章 微软
 - 17.1DOS
 - 17.2IBM兼容
 - 17.3键盘捕获工具
 - 17.4DOS访问控制软件
- 18.9.2IRIX的严重的远程弱点
- 18.9.3SunOS和Solaris的严重的远程弱点
- 18.9.4linux的严重的远程弱点
- 18.10 下一步：检查服务
 - 18.10.1rServices
 - 18.10.2fingerService
 - 18.10.3Telnet
 - 18.10.4FTP
 - 18.10.5常规FTP
 - 18.10.6TFTPD
 - 18.10.7Gopher
 - 18.10.8网络文件系统
 - 18.10.9HTTP
 - 18.10.10保持文件系统的记录
- 18.11关于X
- 18.12检查列表及指南
- 18.13部分UNIX攻击工具
- 18.14出版物和一些其他工具
 - 18.14.1书
 - 18.14.2在线出版物
- 18.15小结
- 第19章 Novell
 - 19.1Novell的内部安全
 - 19.2缺省口令
 - 19.3标识弱点
 - 19.4登录脚本弱点
 - 19.5嗅探器和Novell
 - 19.6NetWare远程攻击
 - 19.7PERL漏洞
 - 19.8登录协议攻击
 - 19.9欺骗
 - 19.10服务拒绝
 - 19.11NovellNetWare4.x上的TCP/IP

服务拒绝

19.12对于服务拒绝攻击的FTP脆弱性

19.13第三方问题

19.14Windows漏洞

19.15WindowsNT漏洞

19.16保护和管理Novell网络的工具

19.16.1审核追踪

19.16.2ProtecNetforNetWare

19.16.3LatticsNet网络管理系统

19.16.4LTAuditort+V6.0

19.16.5NovellNetWareKana安全

分析工具

19.16.6 来自BaselineSoftware公司的

信息安全策略

19.16.7 Me nuWo rks

19.16.8AuditWareforNDS

19.16.9 WSetPass1.55

19.16.10WnSyscon0.95

19.16.11BindViewEMS

19.16.12SecureConsole

19.16.13GETEQUIV.EXE

19.17 破译Novell网络或测试它们安
全性的工具

19.18Getit

19.19Burglar

19.20Spooflog

19.21Setpass

19.22NWPCRAK

19.23IPXCntrl

19.24Crack

19.25Snoop

19.26Novelbfh.exe

19.27其他Novell破译工具

19.28资源

19.28.1资源集合

19.28.2Usenet新闻组

19.28.3书

第20章 VAX/VMS

20.1VMS

20.2VMS的安全性

20.3 一些老的漏洞

20.3.1Mountd漏洞

20.3.2监视器工具的漏洞

20.3.3历史上的问题：Wank蠕虫
事件

20.4 审计与监视

20.4.1watchdog.com

20.4.2Stealth

20.4.3 GUESS__PASSWORD

20.4.4WATCHER

20.4.5 Checkpass

20.4.6Crypt

20.4.7DIAL

20.4.8CALLBACK.EXE

- 20.4.9TCPFLITER (G.Gerard)
- 20.5时代变了
- 20.6小结
- 20.7资源
- 第21章 Macintosh
 - 21.1建立一个MacintoshWeb服务器
 - 21.1.1 WebSTAR的挑战
 - 21.1.2BlueWorld的Lasso
 - 21.1.3挖掘自己的潜能
 - 21.2Macintosh平台的弱点
 - 21.2.1FoolProof弱点
 - 21.2.2由于端口溢出而服务拒绝
 - 21.2.3MacDNS错误
 - 21.2.4 Death序列和WebSTAR
 - 21.2.5 DiskGuard错误
 - 21.2.6 Retrospect弱点
 - 21.2.7AtEase错误
 - 21.2.8NetWorkAssistant
 - 21.2.9MacOS8.0升级版的口令安全性
 - 21.3关于文件共享及安全性
 - 21.3.1服务器管理以及安全性
 - 21.3.2 AGGroup的EtherPeekv.3.5
 - 21.3.3DartmouthSoftwareDevelopment的InterMapper2.0
 - 21.3.4InterlinkComputerSciences公司的NetLock
 - 21.3.5Cyno的MacRansom
 - 21.3.6NetworkSecurityGuard
 - 21.3.7NetworkScout1.0
 - 21.3.8TimbuktuPro4.0
 - 21.3.9内部安全
 - 21.4口令破译以及相关的工具
 - 21.4.1PassFinder
 - 21.4.2FirstClassThrash!
 - 21.4.3FMProPeeker1.1
 - 21.4.4FMPPasswordViewerGold2.0
 - 21.4.5MasterKeyII
 - 21.4.6PasswordKiller
 - 21.4.7KillerCracker
 - 21.4.8MacCrack
 - 21.4.9RemovePasswords
 - 21.4.10Removelt
 - 21.5小结
 - 21.6资源
 - 21.6.1书和报告
 - 21.6.2工具和军需品站点
 - 21.6.3电子杂志和电子在线杂志
- 第五部分 进阶
- 第22章 谁是主管
 - 22.1 一般概念
 - 22.2关于访问控制
 - 22.3关于得到根
 - 22.3.1许可系统的Pros和Cons

- 22.3.2破译根
- 22.4 根也许会成为历史
- 22.5其他操作系统的根
- 22.6 小结
- 第23章 内部安全
- 23.1内部安全
- 23.2我们确实需要内部安全吗
- 23.3为什么内部攻击如此普遍
- 23.4 关于规定
- 23.5硬件考虑
- 23.6驱动器、目录以及文件
- 23.7 一般内部安全评估
- 23.8内部安全扫描器
- 23.8.1SysCAT
- 23.8.2SQLAudidto
- 23.8.3SystemSecurityScanner (S3)
- 23.8.4RSCAN
- 23.9控制雇员访问Internet
- 23.9.1BessSchoolandBusinessFilters
的N2H2
- 23.9.2WebSENSE
- 23.9.3X—STOP
- 23.9.4SequelNetAccessManage
- 23.9.5SmartFilter
- 23.10 开发最实用的核对表
- 23.11 小结
- 第六部分 远程攻击
- 第24章 远程攻击
- 24.1何谓远程攻击
- 24.2第一步骤
- 24.3获取网络概况
- 24.3.1WHOIS
- 24.3.2finger和ruse
- 24.4操作系统
- 24.5考察阶段
- 24.5.1识别系统中的关键弱点
- 24.5.2系统弱点的数据收集
- 24.6进行测试运行
- 24.7小结
- 第25章 攻击级别
- 25.1攻击何时发生
- 25.2破译者使用什么操作系统
- 25.2.1Sun
- 25.2.2UNIX
- 25.2.3Microsoft
- 25.3攻击的起源
- 25.4典型的攻击者是什么样的人
- 25.5典型的目标是什么样子
- 25.6他们为何要攻击
- 25.关于攻击
- 25.8Sams破译级别索引
- 25.8.1敏感级
- 25.8.2响应级
- 25.9小结

- 25.10资源
- 第26章 电子欺骗攻击
 - 26.1什么是电子欺骗
 - 26.2Internet安全基础
 - 26.2.1认证的方法
 - 26.2.2RHOSTS
 - 26.3电子欺骗攻击机制
 - 26.4 一次成功电子欺骗攻击的因素
 - 26.5猜序数
 - 26.5.1打开 个更合适的漏洞
 - 26.5.2谁能受欺骗
 - 26.5.3电子欺骗攻击普遍吗
 - 26.6关于IP电子欺骗的文档
 - 26.7 我们怎样防止IP电子欺骗
 - 26.8其他奇怪和不规则的电子欺骗攻击
 - 26.8.1ARP电子欺骗
 - 26.8.2DNS电子欺骗
 - 26.9小结
- 第27章 基于远程登录攻击
 - 27.1Telnet
 - 27.1.1虚拟终端
 - 27.1.2Telnet安全的历史
 - 27.1.3修改环境
 - 27.1.4终端仿真
 - 27.1.5这些攻击不再有效了吗
 - 27.1.6Telnet作为一种武器
 - 27.2小结
 - 27.3资源
- 第28章 语言、扩展和安全
 - 28.1WWW崛起
 - 28.2CGI和安全
 - 28.2.1实用摘要和报告语言 (Perl)
 - 28.2.2Perl安全
 - 28.2.3特权方式下运行脚本程序的问题
 - 28.2.4文件产生
 - 28.2.5服务器侧includes
 - 28.2.6Java
 - 28.3 ActiveX
 - 28.4 脚本语言
 - 28.4.1Javascript
 - 28.4.2VBScript
 - 28.4.3走近脚本语言
 - 28.5小结
- 第29章 隐藏身份
 - 29.1暴露程度
 - 29.2Web浏览和侵秘
 - 29.2.1Internet与隐私
 - 29.2.2用户信息在服务器上是怎样存储的
 - 29.2.3finger
 - 29.2.4MasterPlan
 - 29.2.5除finger外的其他途径
 - 29.3浏览器的安全件

29.4cookie
29.5用Lucent技术解决隐私问题
29.6用户Email地址和Usenet
29.6.1DejaNews
29.6.2WHOIS服务
29.警告
第七部分 附录
A 安全图书书目——进一步读物
B 如何得到更多信息
C 安全顾问
D 参考文献
E 实质性内容：计算机安全与法律
F CD-ROM上的内容
G 安全术语
• • • • • ([收起](#))

[网络安全技术内幕_下载链接1](#)

标签

网络安全技术内幕

第一人称？

安全

匿名

评论

[网络安全技术内幕_下载链接1](#)

书评

[网络安全技术内幕 下载链接1](#)