
EIAEC
全国信息技术水平考试指定教材
计算机网络信息安全
理论与实践教程
全国电子信息应用教育中心 组编
蒋建春 杨 凡 文伟平 郑生琳 编著
西安电子科技大学出版社
http:// www.xduph. com

全国信息技术水平考试指定教材

计算机网络信息安全理论与实践教程

全国电子信息应用教育中心　　组编

蒋建春　杨　凡　文伟平　郑生琳　编著

西安电子科技大学出版社

2005

内 容 简 介

本书是全国信息技术水平考试“计算机网络信息安全高级技术证书”考试指定教材。

本书共21章，包括网络信息安全基础理论、网络安全技术与标准、网络安全管理实践及网络信息安全实验指导等四大部分。本书针对各种网络安全技术的特点，详细分析了各技术的原理，并给出了典型的应用实例。本书各章还配有思考与练习题，可方便读者学习。

本书集学术、教学和管理于一体，针对当前的各种网络安全问题，总结了一套完整的、科学的、切合实际的网络安全管理流程、网络安全防范体系与安全机制，并把各种具体的网络安全技术纳入其中。

本书是“计算机网络信息安全高级技术证书”水平考试人员的必备教材，也可以作为从事网络信息安全的广大技术人员和大专院校师生的参考用书。

图书在版编目(CIP)数据

计算机网络信息安全理论与实践教程 / 蒋建春等编著.

—西安：西安电子科技大学出版社，2005.9

ISBN 7-5606-1570-8

Ⅰ. 计… Ⅱ. 蒋… Ⅲ. 计算机网络—安全技术—水平考试—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2005)第 107268 号

策　　划　臧延新

责任编辑　阎　彬　臧延新

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　　邮　编　710071

http: //www.xduph.com　　E-mail: xdupfxb@pub.xaonline.com

经　　销　新华书店

印刷单位　陕西画报社印刷厂

版　　次　2005 年 9 月第 1 版　　2005 年 9 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印　张　19.5

字　　数　452 千字

印　　数　1～4000 册

定　　价　32.00 元

ISBN 7-5606-1570-8/TP・0897

XDUP 1861001-1

序

随着信息技术在经济和社会各领域的不断深入应用，信息技术对于生产力乃至人类文明发展的巨大作用越来越明显。党的“十六大”提出，要“优先发展信息产业，在经济和社会领域广泛应用信息技术”。这就明确了我国经济发展的道路，赋予了信息产业新的历史使命。近年来，日新月异的信息技术呈现出新的发展趋势，各类信息技术加快了相互融合和渗透的步伐，信息技术与其他技术的结合更加紧密，信息技术应用的深度、广度和专业化程度也在不断提高，信息技术人才在综合国力的竞争中也越来越占有重要的地位。

为了抓住机遇，迎接挑战，实施人才强国战略，信息产业部启动了“全国信息技术人才培养工程”。该项工程旨在通过政府政策引导，充分发挥全行业和全社会教育培训资源的作用，建立规范的信息技术教育培训体系、科学的培训课程体系和严谨的信息技术人才评测服务体系，培养和造就出大批行业急需的、结构合理的高素质信息技术应用型人才，以促进信息产业持续、快速、协调、健康的发展。

全国信息技术水平考试是根据信息产业部的有关规定，组织并委托信息产业部全国电子信息应用教育中心负责具体实施的全国统一考试，是全国信息技术人才培养工程的重要组成部分，该考试坚持客观公正，中立权威，走国际化道路，以严格的认证质量赢得了社会的认可。

为了配合全国信息技术水平考试，满足信息产业对技术人才素质与能力的需求，在充分吸取国内外先进信息技术培训课程优点的基础上，信息产业部全国电子信息应用教育中心精心组织编写了全国信息技术水平考试用书。这些教材注重提升信息技术人才分析问题和解决问题的能力，对各层次信息技术人才的培养工作具有现实的指导意义。

信息产业部全国电子信息应用教育中心

前　言

目前，许多关系到国计民生的重要信息系统，如金融、电信、电力、交通、医疗卫生、应急、国防、企业等信息系统，都是基于网络而运转的。社会信息化和信息网络化使得信息与网络的价值不断提升。在享受网络带来的方便的同时，网络安全问题也日益增多，网络系统面临着各种不同的安全威胁，如计算机病毒、网络蠕虫、口令破解、协议攻击、特洛伊木马程序、拒绝服务等。因此，网络安全管理的重要性日渐突出。

本书是一本系统论述网络信息安全技术理论与实践的教材，书中总结了常见的网络安全技术以及网络安全管理基本方法，针对各种网络安全技术的特点，详细分析了各技术的原理，并给出了典型的应用实例。同时，本书各章配有思考与练习题，可方便读者学习和理解。

本书共21章，主要内容包括：网络信息安全概论、网络攻击原理与常用方法、网络安全体系、网络安全密码学基本理论、物理与环境安全技术、认证技术的原理与应用、访问控制技术的原理与应用、防火墙技术的原理与应用、VPN 技术的原理与应用、漏洞扫描技术的原理与应用、入侵检测技术的原理与应用、恶意代码防范技术的原理、网络物理隔离技术的原理与应用、网络安全新技术、网络安全技术相关标准、网络安全风险评估技术的原理与应用、Windows 系统安全、UNIX/Linux 操作系统安全、网络路由设备安全、应急响应技术的原理与灾害恢复及实验指导。

在本书的写作与出版过程中，作者得到了中国科学院信息安全技术工程研究中心广大工作人员与研究生的支持和帮助，感谢卿斯汉老师、冯登国老师、倪惜珍老师的悉心指导，感谢马恒太博士、李小满硕士、张涛硕士、王业君硕士、胡振宇博士生的热情帮助。作者同时要感谢网上安全论坛中的网友所提供的资料以及其他各界朋友的支持，由于篇幅所限，所用到的参考文献不能一一列举出来，敬请理解。同时，作者要特别感谢信息产业部电子教育中心盛晨媛女士，在本书写作过程中她给出了许多宝贵的指导意见。

本书是作者在网络安全领域工作中的一次总结，也是一次新的尝试。由于作者水平有限，书中如果有不当之处，希望广大读者不吝赐教。

作　者

2005年7月

目　录

第一篇　网络信息安全基础理论

第 1 章　网络信息安全概论 3
1.1　网络安全现状与问题 3
1.1.1　网络安全现状 3
1.1.2　典型网络安全问题 3
1.2　网络安全目标与功能 4
1.2.1　网络安全目标 4
1.2.2　网络安全基本功能 5
1.3　网络安全技术需求 5
1.3.1　网络物理安全 5
1.3.2　网络认证 6
1.3.3　网络访问控制 6
1.3.4　网络安全保密 6
1.3.5　网络安全监测 6
1.3.6　网络漏洞评估 6
1.3.7　防范网络恶意代码 6
1.3.8　网络安全应急响应 7
1.3.9　网络安全体系 7
1.4　网络安全管理内涵 7
1.4.1　网络安全管理定义 7
1.4.2　网络安全管理的目标 7
1.4.3　网络安全管理的内容 7
1.4.4　网络安全管理要素 7
1.4.5　网络安全管理对象 8
1.4.6　网络安全威胁 8
1.4.7　网络脆弱性 10
1.4.8　网络安全风险 11
1.4.9　网络安全保护措施 11
1.5　网络安全管理方法与流程 11
1.5.1　网络安全管理基本方法 11
1.5.2　网络安全管理基本流程 12
1.6　本章小结 13
本章思考与练习 13

第 2 章　网络攻击原理与常用方法 14
2.1　网络攻击概述 14
2.1.1　网络攻击概念 14
2.1.2　网络攻击技术的发展演变 15
2.2　网络攻击的一般过程 16
2.2.1　隐藏攻击源 16
2.2.2　收集攻击目标信息 17
2.2.3　挖掘漏洞信息 17
2.2.4　获取目标访问权限 18
2.2.5　隐蔽攻击行为 18
2.2.6　实施攻击 18
2.2.7　开辟后门 19
2.2.8　清除攻击痕迹 19
2.3　网络攻击常见技术方法 19
2.3.1　端口扫描 19
2.3.2　口令破解 21
2.3.3　缓冲区溢出 21
2.3.4　网络蠕虫 22
2.3.5　网站假冒 22
2.3.6　拒绝服务 22
2.3.7　网络嗅探 23
2.3.8　SQL 注入攻击 24
2.3.9　社交工程方法(Social Engineering) ... 25
2.3.10　电子监听技术 25
2.3.11　会话劫持 25
2.3.12　漏洞扫描 25
2.3.13　代理技术 26

2.3.14 数据加密技术 26
2.4 黑客常用软件 26
2.4.1 扫描类软件 26
2.4.2 远程监控类软件 27
2.4.3 系统攻击和密码破解 27
2.4.4 监听类软件 28
2.5 网络攻击案例 29
2.5.1 nmap 扫描 29
2.5.2 DDoS 攻击 31
2.5.3 W32.Blaster.Worm 32
2.5.4 网络嗅探攻击 32
2.5.5 MS SQL 数据库攻击 34
2.6 本章小结 39
本章思考与练习 39

第 3 章 网络安全体系 40
3.1 网络安全体系概述 40
3.1.1 网络安全体系概念 40
3.1.2 网络安全体系用途 40
3.1.3 网络安全体系组成 40
3.1.4 网络安全体系模型发展状况 41
3.2 网络安全体系的构建原则与内容 42
3.2.1 网络安全体系建立原则 42
3.2.2 网络安全组织体系构建内容 43
3.2.3 网络安全管理体系构建内容 44
3.2.4 网络安全技术体系构建内容 48
3.3 本章小结 49
本章思考与练习 49

第 4 章 网络安全密码学基本理论 50
4.1 密码学概况 50
4.1.1 密码学发展简况 50
4.1.2 密码学基本概念 50
4.1.3 密码攻击分类与安全 50
4.2 密码体制分类 51
4.2.1 私钥密码体制 51
4.2.2 公钥密码体制 51
4.2.3 混合密码体制 52
4.3 常见密码算法 53
4.3.1 DES 53
4.3.2 IDEA 53
4.3.3 AES 53
4.3.4 RSA 53
4.3.5 Diffie-Hellman 密钥交换协议 54
4.4 杂凑函数 55
4.5 数字签名 56
4.6 安全协议 57
4.6.1 SSL 57
4.6.2 SSH 59
4.7 密码理论的网络安全应用举例 60
4.7.1 路由器安全应用 60
4.7.2 Web 网站安全应用 61
4.7.3 电子邮件安全应用 61
4.8 本章小结 62
本章思考与练习 62

第二篇 网络安全技术与标准

第 5 章 物理与环境安全技术 65
5.1 物理安全概述 65
5.2 物理安全常见方法 66
5.2.1 防火 66
5.2.2 防水 66
5.2.3 防震 66
5.2.4 防盗 67
5.2.5 防鼠虫害 67
5.2.6 防雷 67
5.2.7 防电磁 67
5.2.8 防静电 68
5.2.9 安全供电 68
5.3 网络机房安全 68
5.3.1 网络机房安全等级 68
5.3.2 网络机房场地选择 69
5.3.3 网络机房组成 70
5.4 网络通信安全 70
5.5 存储介质安全 71
5.6 本章小结 71
本章思考与练习 72

第 6 章　认证技术的原理与应用 73
6.1　认证相关概念 73
6.2　认证信息类型 73
6.3　认证的作用和意义 73
6.4　认证方法分类 74
6.4.1　单向认证 74
6.4.2　双向认证 74
6.4.3　第三方认证 75
6.5　认证实现技术 75
6.5.1　口令认证技术 75
6.5.2　智能卡技术 77
6.5.3　基于生物特征认证 77
6.5.4　Kerberos 78
6.5.5　公钥基础设施(PKI) 81
6.5.6　单点登录(Single Logon Schemes) 82
6.6　认证技术应用案例 82
6.6.1　网络接入认证 82
6.6.2　Web 服务器认证 82
6.7　本章小结 82
本章思考与练习 82

第 7 章　访问控制技术的原理与应用 84
7.1　访问控制目标 84
7.2　访问控制系统模型 84
7.3　访问授权和模型 85
7.4　访问控制类型 86
7.4.1　自主访问控制 86
7.4.2　强制访问控制 87
7.4.3　基于角色访问控制 87
7.5　访问控制策略的设计与组成 88
7.5.1　访问控制策略 88
7.5.2　访问控制规则 89
7.5.3　军事安全策略 90
7.6　访问控制管理过程和内容 91
7.6.1　访问控制管理过程 91
7.6.2　最小特权管理 91
7.6.3　用户访问管理 91
7.6.4　口令管理 92
7.7　访问控制案例分析 93
7.7.1　UNIX/Linux 系统访问控制案例 93
7.7.2　Windows 2000 访问控制案例 93
7.7.3　IIS-FTP 访问控制案例 94
7.7.4　网络访问控制案例 95
7.7.5　Web 访问控制案例 96
7.8　本章小结 98
本章思考与练习 98

第 8 章　防火墙技术的原理与应用 99
8.1　防火墙概述 99
8.1.1　防火墙技术背景 99
8.1.2　防火墙工作原理 99
8.1.3　防火墙缺陷 101
8.2　防火墙技术与类型 101
8.2.1　包过滤 101
8.2.2　应用服务代理 103
8.2.3　网络地址转换 105
8.3　防火墙主要技术参数 106
8.3.1　防火墙功能指标 106
8.3.2　防火墙性能指标 106
8.3.3　防火墙安全指标 107
8.4　防火墙防御体系结构类型 107
8.4.1　基于双宿主主机防火墙结构 107
8.4.2　基于代理型防火墙结构 107
8.4.3　基于屏蔽子网的防火墙结构 108
8.5　防火墙部署与应用案例 109
8.5.1　防火墙部署的基本方法与步骤 109
8.5.2　基于 Cisco 路由器的安全应用案例 109
8.6　本章小结 112
本章思考与练习 112

第 9 章　VPN 技术的原理与应用 113
9.1　VPN 概况 113
9.1.1　VPN 概念 113
9.1.2　VPN 安全服务功能 113
9.1.3　VPN 实现方式 113
9.2　VPN 相关技术 114
9.2.1　密码算法 114

9.2.2 密钥管理 114
9.2.3 认证访问控制 114
9.2.4 IPSec 114
9.2.5 PPTP 116
9.3 VPN 典型应用 116
9.3.1 VPN 应用类型概况 116
9.3.2 Access VPN 116
9.3.3 Intranet VPN 116
9.3.4 Extranet VPN 117
9.4 本章小结 117
本章思考与练习 117

第 10 章 漏洞扫描技术的原理与应用 118
10.1 网络系统漏洞概述 118
10.1.1 漏洞概念 118
10.1.2 漏洞与网络安全 118
10.1.3 网络系统漏洞来源 119
10.1.4 网络系统漏洞发布机制 119
10.1.5 网络系统漏洞信息公布网址 120
10.2 漏洞扫描技术 121
10.3 漏洞扫描器组成结构 122
10.4 常用网络漏洞扫描工具 122
10.4.1 COPS 122
10.4.2 SAINT 124
10.4.3 Nessus 124
10.4.5 LANguard 网络扫描器 125
10.4.6 X-scan 125
10.4.7 Whisker 125
10.5 漏洞扫描器安装模式及实例 125
10.5.1 漏洞扫描器安装模式 125
10.5.2 Windows 系统漏洞扫描实例 126
10.5.3 CGI 漏洞扫描 126
10.6 本章小结 127
本章思考与练习 127

第 11 章 入侵检测技术的原理与应用 128
11.1 入侵检测概述 128
11.1.1 入侵检测概念 128
11.1.2 入侵检测系统模型 128
11.1.3 入侵检测作用 129
11.2 入侵检测技术 129
11.2.1 基于误用的入侵检测技术 129
11.2.2 基于异常的入侵检测技术 130
11.2.3 其他 133
11.3 入侵检测系统的组成与分类 133
11.3.1 入侵检测系统的组成 133
11.3.2 基于主机的入侵检测系统 134
11.3.3 基于网络的入侵检测系统 135
11.3.4 分布式入侵检测系统 137
11.4 入侵检测系统的评估指标 138
11.5 入侵检测系统的部署方法与应用案例 139
11.5.1 IDS 的部署方法与步骤 139
11.5.2 HIDS 应用实例 139
11.5.3 NIDS 应用实例 140
11.6 本章小结 140
本章思考与练习 141

第 12 章 恶意代码防范技术的原理 142
12.1 恶意代码概述 142
12.1.1 恶意代码的定义与分类 142
12.1.2 恶意代码防范整体策略 143
12.2 计算机病毒 143
12.2.1 计算机病毒的概念与特性 143
12.2.2 计算机病毒的组成与运行机制 145
12.2.3 计算机病毒常见类型与技术 145
12.2.4 计算机病毒防范策略与技术 146
12.2.5 计算机病毒防御模式 148
12.3 特洛伊木马 150
12.3.1 特洛伊木马的概念与特性 150
12.3.2 特洛伊木马的运行机制 150
12.3.3 特洛伊木马技术 151
12.3.4 伊木马防范技术 153
12.4 网络蠕虫 155
12.4.1 网络蠕虫的概念与特性 155
12.4.2 网络蠕虫的组成与运行机制 156

12.4.3 网络蠕虫常用技术 157
12.4.4 网络蠕虫防范技术 159
12.5 其他恶意代码 161
12.5.1 逻辑炸弹(Logic Bombs) 161
12.5.2 陷门(Trapdoors) 161
12.5.3 细菌(Bacteria) 161
12.5.4 间谍软件(Spyware) 161
12.6 本章小结 162
本章思考与练习 162

第 13 章 网络物理隔离技术的原理与应用 163
13.1 网络物理隔离概况 163
13.2 网络物理隔离技术 163
13.2.1 专用计算机上网 163
13.2.2 多 PC 机 163
13.2.3 外网代理服务 164
13.2.4 内外网线路切换器 164
13.2.5 单硬盘内外分区 164
13.2.6 双硬盘 165
13.2.7 网闸 165
13.3 网络物理隔离典型应用案例 166
13.3.1 工作机安全上网实例 166
13.3.2 电子政务中网闸应用实例 167
13.4 本章小结 167
本章思考与练习 168

第 14 章 网络安全新技术 169
14.1 入侵阻断 169
14.2 网络攻击诱骗 170
14.3 网络攻击容忍和系统生存 173
14.4 可信计算 174
14.5 本章小结 175
本章思考与练习 175

第 15 章 网络安全技术相关标准 176
15.1 安全标准概况 176
15.2 TCSEC 176
15.3 GB 17859 177
15.3.1 第一级：用户自主保护级 178
15.3.2 第二级：系统审计保护级 178
15.3.3 第三级：安全标记保护级 178
15.3.4 第四级：结构化保护级 179
15.3.5 第五级：访问验证保护级 179
15.4 CC 标准 179
15.4.1 CC 标准概况 179
15.4.2 CC 的开发目的和应用范围 180
15.4.3 CC 标准组成 180
15.4.4 CC 标准的目标读者 181
15.5 BS7799 181
15.6 本章小结 182
本章思考与练习 182

第三篇 网络安全管理实践

第 16 章 网络安全风险评估技术的原理与应用 185
16.1 网络风险评估概述 185
16.1.1 网络风险评估的概念 185
16.1.2 网络风险评估要素的组成关系 185
16.1.3 网络风险评估模式 186
16.1.4 网络风险评估意义 186
16.2 网络风险评估过程 187
16.2.1 风险评估过程概述 187
16.2.2 网络评估范围界定 187
16.2.3 网络资产鉴定 188
16.2.4 网络威胁识别 188
16.2.5 网络脆弱性识别 190
16.2.6 网络安全措施分析 190
16.2.7 网络安全影响分析 190
16.2.8 网络风险确认 190
16.2.9 网络安全措施建议 190
16.3 网络风险数据的采集方法与工具 191
16.3.1 漏洞扫描 191
16.3.2 人工检查 192

16.3.3 渗透测试 192
16.3.4 问卷调查 192
16.3.5 安全访谈 193
16.3.6 审计数据分析 193
16.3.7 入侵监测 194
16.4 网络风险评估工程项目流程 194
16.4.1 评估工程的前期准备 194
16.4.2 评估方案的设计与论证 195
16.4.3 评估方案的实施 195
16.4.4 风险评估报告的撰写 195
16.4.5 评估结果的评审与认可 195
16.5 本章小结 196
本章思考与练习 196

第 17 章 Windows 系统安全 197
17.1 Windows 系统安全概况 197
17.1.1 Windows 系统架构 197
17.1.2 Windows 安全模型 198
17.1.3 Windows 安全机制 198
17.2 Windows 系统安全分析 199
17.2.1 Windows 口令 199
17.2.2 Windows 恶意代码 199
17.2.3 Windows 应用软件漏洞 200
17.2.4 Windows 系统程序的漏洞 200
17.2.5 Windows 注册表安全 200
17.2.6 Windows 文件共享安全 200
17.2.7 Windows 物理临近攻击 200
17.3 Windows 系统安全增强技术方法与流程 200
17.3.1 Windows 系统安全增强方法概述 200
17.3.2 Windows 系统安全增强基本流程 201
17.4 Windows 2000 系统安全增强实例 202
17.4.1 系统启动安全增强 202
17.4.2 帐号与口令管理安全增强 203
17.4.3 安装最新系统补丁 204
17.4.4 网络安全增强 204
17.4.5 安装第三方防护软件 205
17.5 Windows 系统常见漏洞与解决方法 205
17.5.1 Unicode 漏洞 205
17.5.2 ISAPI 缓冲区扩展溢出 206
17.5.3 IIS RDS(Microsoft Remote Data Services) 206
17.5.4 NetBIOS 207
17.5.5 空对话连接造成的信息泄露 207
17.5.6 SAM 中的弱散列(LM hash) 208
17.6 本章小结 208
本章思考与练习 209

第 18 章 UNIX/Linux 操作系统安全 210
18.1 UNIX/Linux 系统安全概况 210
18.1.1 UNIX/Linux 系统结构 210
18.1.2 UNIX/Linux 安全机制 210
18.2 UNIX/Linux 系统安全分析 211
18.2.1 UNIX/Linux 口令/帐号安全 211
18.2.2 UNIX/Linux 可信主机文件安全 212
18.2.3 UNIX/Linux 应用软件漏洞 212
18.2.4 UNIX/Linux 的 SUID 文件安全 212
18.2.5 UNIX/Linux 的恶意代码 212
18.2.6 UNIX/Linux 文件系统安全 212
18.2.7 UNIX/Linux 网络服务安全 212
18.2.8 UNIX/Linux 系统程序漏洞 213
18.3 UNIX/Linux 系统安全增强方法和流程 213
18.3.1 UNIX/Linux 系统安全增强方法 213
18.3.2 UNIX/Linux 系统安全增强基本流程 213
18.4 UNIX/Linux 系统安全增强技术 214
18.4.1 安装系统补丁软件包 214
18.4.2 最小化系统网络服务 215
18.4.3 设置系统开机保护口令 215
18.4.4 弱口令检查 215
18.4.5 禁用默认帐号 217
18.4.6 用 SSH 增强网络服务安全 217
18.4.7 利用 tcp_wrapper 增强访问控制 217

18.4.8 构筑 UNIX/Linux 主机防火墙.....217
18.4.9 使用 Tripwire 或 md5sum 完整性检测工具.....217
18.4.10 检测 LKM 后门.....217
18.4.11 系统安全监测.....218
18.5 Linux 安全增强实例.....218
18.6 UNIX/Linux 系统常见漏洞与解决方法.....220
18.6.1 空口令或弱口令的帐号.....220
18.6.2 r 命令.....220
18.6.3 RPC 服务缓冲区溢出.....221
18.6.4 缺省 SNMP 字串.....221
18.6.5 Sendmail.....222
18.6.6 LPD.....222
18.6.7 sadmind and mountd.....223
18.7 本章小结.....223
本章思考与练习.....223

第 19 章 网络路由设备安全.....224
19.1 路由器安全概述.....224
19.1.1 路由器安全威胁.....224
19.1.2 路由器安全结构.....224
19.1.3 路由器安全策略.....225
19.2 路由器物理安全.....226
19.3 路由器访问安全.....226
19.3.1 本地访问安全.....226
19.3.2 远程访问安全.....226
19.4 路由器的网络服务安全.....227
19.5 路由信息及协议安全.....229
19.6 路由器审计和管理.....231
19.7 路由器安全测试方法与工具.....232
19.7.1 路由器安全功能测试.....232
19.7.2 路由器抗攻击测试.....232
19.7.3 路由器漏洞扫描.....232
19.8 路由器安全管理增强技术方法.....233
19.8.1 及时升级操作系统和打补丁.....233
19.8.2 关闭不需要的网络服务及接口.....233
19.8.3 禁止 IP 直接广播和源路由.....233
19.8.4 增强路由器 VTY 安全.....233
19.8.5 阻断恶意数据包.....234
19.8.6 路由器口令安全.....234
19.8.7 传输加密.....234
19.9 Cisco 路由器常见漏洞与解决方法.....235
19.9.1 Cisco IOS 畸形 MPLS 包远程拒绝服务漏洞.....235
19.9.2 Cisco IOS 畸形 BGP 包远程拒绝服务漏洞.....235
19.9.3 Cisco Telnet 远程拒绝服务漏洞.....235
19.9.4 Cisco Secure Access Control Server ACS GUI 验证绕过漏洞.....236
19.9.5 Cisco Secure ACS LEAP RADIUS 代理远程拒绝服务漏洞.....236
19.9.6 Cisco IOS 畸形 OSPF 包远程拒绝服务漏洞.....236
19.9.7 Cisco IOS OSPF 路由表破坏漏洞.....236
19.9.8 Cisco IOS 畸形 BGP 数据包设备可导致设备复位漏洞.....237
19.10 本章小结.....237
本章思考与练习.....237

第 20 章 应急响应技术的原理与灾害恢复.....238
20.1 应急响应概念.....238
20.2 应急小组组成与工作机制.....238
20.2.1 应急小组组成.....238
20.2.2 应急小组工作机制.....238
20.2.3 应急小组组成模式.....239
20.3 应急方案.....241
20.3.1 应急方案内容.....241
20.3.2 应急方案类型.....241
20.4 应急事件处理流程.....241
20.5 应急响应技术与常见实用软件.....242
20.5.1 应急响应技术类型.....242
20.5.2 访问控制.....243
20.5.3 安全状态评估.....243
20.5.4 系统监测.....244
20.5.5 系统恢复.....244

20.5.6 入侵取证 245
20.6 应急响应案例分析 245
20.6.1 Windows 口令丢失恢复 245
20.6.2 硬盘数据恢复 246
20.7 本章小结 246
本章思考与习题 246

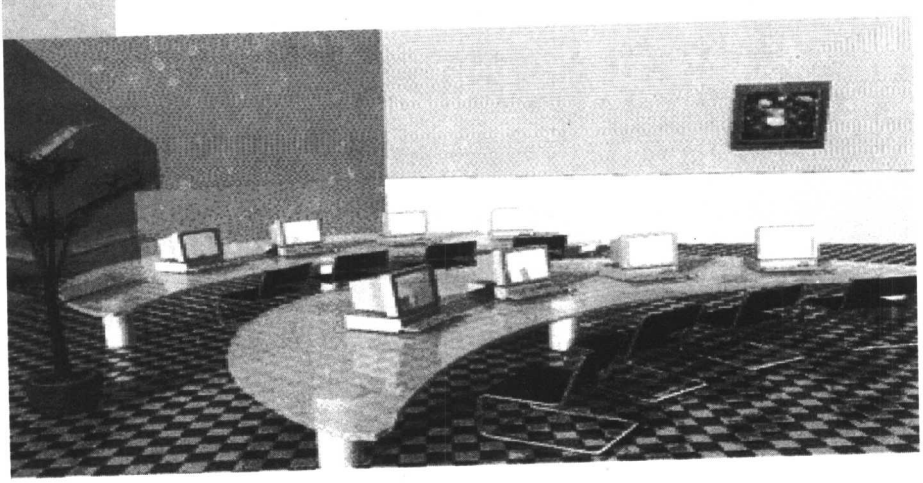
第四篇 网络信息安全实验指导

第 21 章 实验指导 249
21.1 操作系统弱口令检测软件的安装和使用 249
21.1.1 实验目的 249
21.1.2 设备需求 249
21.1.3 实验环境及配置说明 249
21.1.4 实验内容 250
21.2 网络漏洞扫描软件 Nessus 的安装和使用 254
21.2.1 实验目的 254
21.2.2 设备需求 254
21.2.3 实验环境及配置说明 254
21.2.4 实验内容 254
21.3 OpenSSH 的安装及使用 260
21.3.1 实验目的 260
21.3.2 设备需求 260
21.3.3 实验环境及配置说明 260
21.3.4 实验内容 261
21.4 邮件加密软件 PGP 的安装和使用 266
21.4.1 实验目的 266
21.4.2 设备需求 267
21.4.3 实验环境及配置说明 267
21.4.4 实验内容 267
21.5 Apache 服务器和 SSL 软件的安装和使用 274
21.5.1 实验目的 274
21.5.2 设备需求 274
21.5.3 实验环境及配置说明 274
21.5.4 实验内容 275
21.6 Linux 防火墙软件 Iptables 的安装和使用 277
21.6.1 实验目的 277
21.6.2 设备需求 277
21.6.3 实验环境及配置说明 277
21.6.4 实验内容 277
21.7 网络入侵检测系统 snort 的安装和使用 278
21.7.1 实验目的 278
21.7.2 设备需求 278
21.7.3 实验环境及配置说明 279
21.7.4 实验内容 279
21.8 常见木马的检测、清除方法和工具的使用 280
21.8.1 实验目的 280
21.8.2 设备需求 280
21.8.3 实验环境及配置说明 280
21.8.4 实验内容 280
21.9 Windump 软件的安装和使用 285
21.9.1 实验目的 285
21.9.2 设备需求 285
21.9.3 实验环境及配置说明 285
21.9.4 实验内容 286
21.10 Windows 2000 系统安全增强 288
21.10.1 实验目的 288
21.10.2 设备需求 288
21.10.3 实验环境及配置说明 289
21.10.4 实验内容 289
21.11 Windows 下 VPN 环境的搭建 291
21.11.1 实验目的 291
21.11.2 设备需求 291
21.11.3 实验环境及配置说明 291
21.11.4 实验内容 292

参考文献 297

第一篇

网络信息安全基础理论



第 1 章

网络信息安全概论

1.1　网络安全现状与问题

1.1.1　网络安全现状

随着信息化建设的发展，网络已经成为支撑许多行业开展业务的基础平台，网络安全将直接影响到业务的正常运转，甚至关系到国家的安全和社会的稳定。目前，网络面临着不同动机的威胁者发动的不同类型的攻击。信息泄露、恶意代码、垃圾邮件、网络恐怖主义等都将影响到网络安全。多协议、多系统、多应用、多用户组成的网络环境，复杂性高，存在难以避免的安全脆弱性。Securityfocus 公司的漏洞统计数据表明，绝大部分操作系统存在安全漏洞。由于管理、软件工程难度等问题，新的安全脆弱点不断地引入到网络环境中，所有这些安全脆弱点都将可能成为攻击的切入点，攻击者可以利用这些脆弱点入侵系统，窃取信息。1998 年 2 月份，黑客利用 Solar Sunrise 弱点入侵美国国防部网络，受害的计算机数超过 500 台，而攻击者只是采用了中等复杂工具。根据美国的 CERT 安全事件统计数据可得安全事件变化趋势图，如图 1-1 所示。

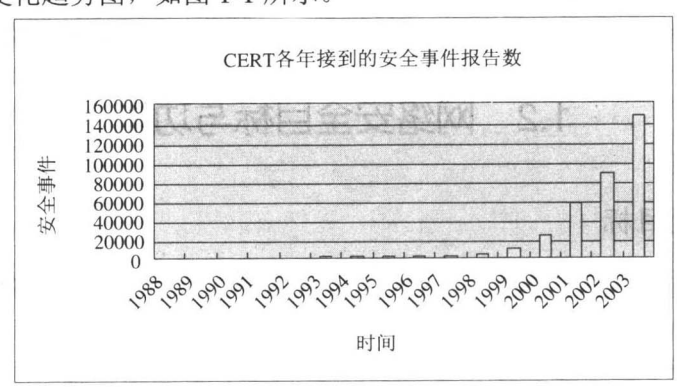


图 1-1　CERT 网络安全事件变化趋势图

1.1.2　典型网络安全问题

目前，主要有 10 个方面的网络安全问题急需解决，分别叙述如下：

(1) 信息应用系统与网络的关系日益紧密，人们对网络的依赖性增强，因而网络安全的影响范围日益扩大，建立可信的网络信息环境已成为一个迫切的需求。

(2) 网络系统中安全漏洞日益增多，不仅技术上有漏洞，管理上也有漏洞。

(3) 恶意代码危害性高。恶意代码通过网络途径广泛扩散，其影响越来越大。

(4) 网络攻击技术日趋复杂，而攻击操作容易完成，攻击工具广为流行。

(5) 网络安全建设缺乏规范操作，常常采取“亡羊补牢”的方式进行维护，导致信息安全共享难度递增，并留下安全隐患。

(6) 网络系统有着种类繁多的安全认证方式，一方面使得用户应用时不方便，另一方面也增加了安全管理的工作难度。

(7) 国内信息化技术严重依赖国外，从硬件到软件都不同程度地受制于人。

(8) 网络系统中软硬件产品的单一性，易造成大规模网络安全事件的发生，特别是网络蠕虫安全事件的发生。

(9) 网络安全建设涉及人员众多，安全和易用性特别难以平衡。

(10) 网络安全管理问题依然是一个难题，主要有：

- 用户信息安全防范意识不强。例如，选取弱口令，使得攻击者从远程即可直接控制主机。
- 网络服务配置不当，开放了过多的网络服务。例如，网络边界没有过滤掉恶意数据包或切断网络连接，允许外部网络的主机直接 ping 内部网主机，允许建立空连接。
- 安装有漏洞的软件包。
- 缺省配置。例如，网络设备的口令直接用厂家的缺省配置。
- 网络系统中软件不打补丁或补丁不全。
- 网络安全敏感信息泄露。例如 DNS 服务信息泄露。
- 网络安全防范缺乏体系。
- 网络信息资产不明，缺乏分类、分级处理。
- 网络安全管理信息单一，缺乏统一分析与管理平台。
- 重技术，轻管理。例如，没有明确的安全管理策略、安全组织及安全规范。

1.2 网络安全目标与功能

1.2.1 网络安全目标

网络安全目标就是五个基本安全属性，即机密性、完整性、可用性、抗抵赖性和可控性。

1. 机密性

网络机密性是指网上资源不泄露给非授权的用户、实体或程序，能够防止网上用户非授权获取网上资源。例如，网络系统上传递的信息有些属于重要安全信息，若一旦攻击者通过监听手段获取到，就有可能危及到网络系统的整体安全，例如网络管理帐号、口令信息等。

2. 完整性

完整性是指网上信息或系统未经授权不能进行更改的特性。例如，网上信息在存储或传输过程中保持不被删除、修改、伪造、插入等的特性。