

<<黑客>>

图书基本信息

书名：<<黑客>>

13位ISBN编号：9787505374355

10位ISBN编号：7505374354

出版时间：2002-1

出版时间：电子工业出版社

作者：(美)eric cole

页数：574

字数：923

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

内容概要

本书全面、系统地介绍了关于网络安全技术的知识和相关问题。

书中主要介绍了能够成功保护网络系统免受攻击的方法，并且对各种攻击的机理进行了全面的论述。

本书的突出特点：全面跟踪了当前黑客攻击的关键技术和方法，针对不同对象和情况，提出了不同的防范策略，具有很强的实用性和时效性。

本书结构合理、内容翔实，有助于训练安全方面的专门人才，使他们能够更好地对各种威胁做出正确的反应，使防范工作做在攻击者的前面。

本书还可以为网络管理员、系统管理员在预防黑客方面提供有效的安全防范与管理策略。

作者简介

Eric Cole曾是美国中央情报局的雇员，现为SANS（系统管理、网络互联和安全研究机构）的高级发言人。

他拥有纽约技术学院的理科学士和理科硕士学位，现在正在攻读网络安全博士学位，专攻入侵检测与隐蔽技术。

Eric Cole在信息安全的诸多方面都有着广泛的经验，其中包括加密技术、隐蔽技术、入侵检测、NT安全、UNIX安全、TCP/IP和网络安全、因特网安全、路由器安全、安全评估、渗透试验、防火墙、安全的Web事务处理、电子商务、SSL、IPSEC以及信息战等。

他是SANS的高级讲师，开设了多门课程，同时针对不同的课题做过系列演讲。

Eric Cole还在纽约技术学院教学，同时担任乔治镇大学的助教。

他还创办了Teligent公司，并兼任该公司安全部门的领导。

书籍目录

- 第1章 简介 1
 - 1.1 进行攻击的黄金时期 1
 - 1.2 问题的严重程度 2
 - 1.2.1 总的趋势 3
 - 1.2.2 为什么问题变得如此严重 7
 - 1.3 公司正在做什么 9
 - 1.3.1 零忍耐 9
 - 1.3.2 侥幸的安全意识 10
 - 1.3.3 试着修复已经建立起来的系统 10
 - 1.3.4 过于重视或者极不重视 11
 - 1.4 公司现在应该做些什么 11
 - 1.4.1 预防和检测投资 11
 - 1.4.2 给予监测技术更多的关注 12
 - 1.4.3 注意对员工的培训 14
 - 1.5 深度防御 14
 - 1.6 本书的目的 14
 - 1.7 合法的使用 15
 - 1.8 本书的内容 15
 - 1.9 小结 16
- 第2章 攻击目的和方法 17
 - 2.1 什么是攻击行为 17
 - 2.2 攻击的步骤 18
 - 2.2.1 被动的侦察 19
 - 2.2.2 主动的侦察 20
 - 2.2.3 入侵系统 21
 - 2.2.4 上传程序 24
 - 2.2.5 下载数据 24
 - 2.2.6 保持访问 24
 - 2.2.7 隐藏踪迹 25
 - 2.3 攻击的种类 26
 - 2.4 入侵行为的种类 27
 - 2.4.1 在Internet上 27
 - 2.4.2 在局域网上 29
 - 2.4.3 本地 33
 - 2.4.4 离线 35
 - 2.5 攻击者进入的途径 37
 - 2.5.1 端口 37
 - 2.5.2 服务 39
 - 2.5.3 第三方软件 40
 - 2.5.4 操作系统 41
 - 2.5.5 口令 42
 - 2.5.6 社会工程 42
 - 2.5.7 特洛伊木马 43
 - 2.5.8 推论引导 43
 - 2.5.9 秘密通道 43

<<黑客>>

- 2.6 攻击者想要达到的目标 44
 - 2.6.1 机密性 44
 - 2.6.2 完整性 45
 - 2.6.3 可用性 45
- 2.7 小结 45
- 第3章 信息搜集 46
 - 3.1 信息搜集的步骤 46
 - 3.1.1 找到初始信息 47
 - 3.1.2 找到网络的地址范围 52
 - 3.1.3 找到活动的机器 57
 - 3.1.4 找到开放端口和入口点 59
 - 3.1.5 弄清操作系统 62
 - 3.1.6 弄清每个端口运行的服务 64
 - 3.1.7 画出网络图 65
 - 3.2 信息搜集总结 67
 - 3.3 实际应用 67
 - 3.3.1 Whois 68
 - 3.3.2 Nslookup 69
 - 3.3.3 ARIN Web Search 70
 - 3.3.4 Traceroute 71
 - 3.3.5 Ping 73
 - 3.3.6 绘制网络图 75
 - 3.3.7 端口扫描和指纹鉴别 75
 - 3.3.8 攻击系统 77
 - 3.4 小结 77
- 第4章 欺骗 78
 - 4.1 欺骗的理由 78
 - 4.2 欺骗的类型 78
 - 4.2.1 IP 欺骗 79
 - 4.2.2 电子邮件欺骗 87
 - 4.2.3 Web 欺骗 92
 - 4.2.4 非技术欺骗 104
 - 4.3 小结 108
- 第5章 会话劫持 109
 - 5.1 欺骗和劫持 109
 - 5.2 会话劫持的种类 110
 - 5.3 TCP/IP 概念 111
 - 5.3.1 TCP 111
 - 5.4 会话劫持的细节 113
 - 5.4.1 发现目标 114
 - 5.4.2 执行顺序预测 114
 - 5.4.3 寻找一个动态的会话 116
 - 5.4.4 猜测序列号 116
 - 5.4.5 使对方下线 116
 - 5.4.6 接管会话 117
 - 5.5 ACK 风暴 117
 - 5.6 会话劫持攻击的程序 117

<<黑客>>

- 5.6.1 Juggernaut 118
- 5.6.2 Hunt 127
- 5.6.3 TTY Watcher 133
- 5.6.4 IP Watcher 134
- 5.7 劫持攻击的危害 134
 - 5.7.1 大多数计算机都易受攻击 135
 - 5.7.2 没有较成功的防范措施 135
 - 5.7.3 劫持攻击非常简单 135
 - 5.7.4 劫持攻击非常危险 135
 - 5.7.5 大多数反劫持攻击方法都不起作用 136
- 5.8 会话劫持攻击的防范措施 136
 - 5.8.1 进行加密 136
 - 5.8.2 使用安全协议 137
 - 5.8.3 限制引入连接 137
 - 5.8.4 减少远端连入 137
 - 5.8.5 拥有完善的认证措施 137
- 5.9 小结 137
- 第6章 拒绝服务攻击 139
 - 6.1 拒绝服务攻击的概念 139
 - 6.1.1 拒绝服务攻击的类型 139
 - 6.2 分布式拒绝服务攻击的概念 140
 - 6.3 难以防范的原因 141
 - 6.4 拒绝服务攻击类型 142
 - 6.4.1 Ping of Death 142
 - 6.4.2 SSPing 145
 - 6.4.3 Land攻击 147
 - 6.4.4 Smurf 149
 - 6.4.5 SYN Flood 152
 - 6.4.6 CPU Hog 155
 - 6.4.7 Win Nuke 157
 - 6.4.8 RPC Locator 160
 - 6.4.9 Jolt2 163
 - 6.4.10 Bubonic 168
 - 6.4.11 Microsoft不完整TCP/IP数据包的脆弱性 172
 - 6.4.12 HP Openview节点管理器SNMP DOS的脆弱性 172
 - 6.4.13 NetScreen防火墙DOS的脆弱性 173
 - 6.4.14 Checkpoint防火墙DOS的脆弱性 174
 - 6.5 DOS攻击工具 175
 - 6.5.1 Targa 175
 - 6.6 DDOS攻击工具 176
 - 6.6.1 TFN2K 177
 - 6.6.2 Trinoo 179
 - 6.6.3 Stacheldraht 181
 - 6.7 防范拒绝服务攻击 181
 - 6.7.1 有效完善的设计 182
 - 6.7.2 带宽限制 182
 - 6.7.3 及时给系统安装补丁 182

<<黑客>>

- 6.7.4 运行尽可能少的服务 182
- 6.7.5 只允许必要的通信 183
- 6.7.6 封锁敌意IP地址 183
- 6.8 防范分布式拒绝服务攻击 183
 - 6.8.1 保持网络安全 184
 - 6.8.2 安装入侵检测系统 184
 - 6.8.3 使用扫描工具 185
 - 6.8.4 运行Zombie工具 186
- 6.9 小结 186
- 第7章 缓冲区溢出攻击 187
 - 7.1 缓冲区溢出攻击的概念 187
 - 7.2 缓冲区溢出的细节 188
 - 7.3 缓冲区溢出攻击类型 190
 - 7.4 存在大量易受攻击程序的原因 190
 - 7.5 缓冲区溢出样例 191
 - 7.6 如何保护例子程序 191
 - 7.7 十种缓冲区溢出攻击 192
 - 7.7.1 NetMeeting缓冲区溢出 192
 - 7.7.2 Outlook缓冲区溢出 196
 - 7.7.3 Linuxconf缓冲区溢出 200
 - 7.7.4 ToolTalk缓冲区溢出 204
 - 7.7.5 IMAPD缓冲区溢出 206
 - 7.7.6 AOL Instant Messenger缓冲区溢出 209
 - 7.7.7 AOL Instant Messenger BuddyIcon缓冲区溢出 210
 - 7.7.8 Microsoft Windows 2000 ActiveX控件缓冲区溢出 211
 - 7.7.9 IIS 4.0/5.0 Phone Book服务器缓冲区溢出 212
 - 7.7.10 SQL Server 2000 扩展存储程序缓冲区溢出 214
 - 7.8 防范缓冲区溢出攻击 217
 - 7.8.1 关闭端口或服务 217
 - 7.8.2 安装厂商的补丁 217
 - 7.8.3 在防火墙上过滤特殊通信 218
 - 7.8.4 检查关键程序 218
 - 7.8.5 以需要的最少权限运行软件 218
 - 7.9 小结 218
- 第8章 口令安全 219
 - 8.1 典型攻击 219
 - 8.2 口令现状 220
 - 8.3 口令的历史 221
 - 8.4 口令的未来 222
 - 8.5 口令管理 224
 - 8.5.1 口令的必要性 224
 - 8.5.2 口令策略的必要性 225
 - 8.5.3 强口令的概念 225
 - 8.5.4 选取强口令的方法 226
 - 8.5.5 保护口令的方法 226
 - 8.6 口令攻击 229
 - 8.6.1 口令破解的概念 229

<<黑客>>

- 8.6.2 口令破解的重要性 231
- 8.6.3 口令攻击的类型 233
- 8.6.4 其他攻击类型 235
- 8.7 小结 236
- 第9章 Microsoft NT 口令破解 238
 - 9.1 NT中口令的存放 238
 - 9.2 破解NT口令的方法 239
 - 9.3 所有的口令都能破解 239
 - 9.3.1 LAN 管理器哈希 239
 - 9.3.2 没有添加成分 240
 - 9.4 NT口令破解程序 241
 - 9.4.1 L0phcrack 241
 - 9.4.2 NTSweep 251
 - 9.4.3 NTCrack 253
 - 9.4.4 PWDump2 254
 - 9.5 比较 254
 - 9.6 提取口令哈希 255
 - 9.7 预防NT 口令破解 255
 - 9.7.1 禁用LAN 管理器认证 256
 - 9.7.2 贯彻强口令 258
 - 9.7.3 拥有强口令策略 259
 - 9.7.4 使用SYSKEY 260
 - 9.7.5 使用一次性口令 261
 - 9.7.6 使用生物技术 261
 - 9.7.7 审计关键文件访问 262
 - 9.7.8 搜索破解工具 262
 - 9.7.9 保存活动账号清单 262
 - 9.7.10 限制拥有域管理员权限的用户 262
 - 9.8 小结 263
- 第10章 UNIX口令破解 264
 - 10.1 UNIX中口令的存放 264
 - 10.1.1 Shadow文件 266
 - 10.2 UNIX加密口令的方法 267
 - 10.3 UNIX 口令破解程序 269
 - 10.3.1 Crack 269
 - 10.3.2 John the Ripper 277
 - 10.3.3 XIT 281
 - 10.3.4 Slurpie 283
 - 10.4 比较 285
 - 10.5 防止 UNIX口令破解 287
 - 10.5.1 采用强口令策略 287
 - 10.5.2 使用Shadow文件 288
 - 10.5.3 使用一次性口令 288
 - 10.5.4 使用生物技术 289
 - 10.5.5 使用Passwd+以实现强口令 289
 - 10.5.6 审计关键文件访问 290
 - 10.5.7 扫描破解工具 290

<<黑客>>

- 10.5.8 保存活动账号清单 290
- 10.5.9 限制拥有根权限的用户 290
- 10.6 小结 290
- 第11章 Microsoft NT基础 291
 - 11.1 NT安全概述 291
 - 11.2 源代码可用性 292
 - 11.3 NT基础 293
 - 11.3.1 NT的组织方式 294
 - 11.3.2 物理安全 295
 - 11.3.3 注册表 295
 - 11.3.4 运行的服务 299
 - 11.3.5 账号管理 300
 - 11.3.6 网络设置 300
 - 11.3.7 审计 303
 - 11.3.8 NetBIOS 306
 - 11.3.9 服务包 307
 - 11.3.10 资源工具箱 307
 - 11.3.11 系统增强指导 312
 - 11.4 小结 312
- 第12章 NT攻击 313
 - 12.1 NT攻击工具 313
 - 12.1.1 GetAdmin 314
 - 12.1.2 SecHole 317
 - 12.1.3 Red Button 320
 - 12.1.4 Microsoft IIS中的RDS安全漏洞 322
 - 12.1.5 Microsoft Shares 327
 - 12.1.6 Legion 332
 - 12.1.7 相对Shell路径弱点 345
 - 12.1.8 使用ODBC数据源工具拦截NT DSN 348
 - 12.1.9 Winfreeze 354
 - 12.1.10 Microsoft Windows媒体播放器JavaScript URL弱点 355
 - 12.1.11 Microsoft Internet Explorer Mstask.exe CPU占用弱点 356
 - 12.1.12 Microsoft MSHTML.DLL崩溃弱点 357
 - 12.1.13 2001 IIS 5.0 允许文件浏览 358
 - 12.1.14 媒体播放器7和IE Java弱点 358
 - 12.1.15 IE 5.x/Outlook 允许执行任何程序 360
 - 12.1.16 IIS 5.0允许执行任何网站服务器命令 361
 - 12.1.17 Microsoft WINS域控制器欺骗弱点 362
 - 12.2 小结 363
- 第13章 UNIX基础 364
 - 13.1 Linux 364
 - 13.2 UNIX的弱点 364
 - 13.2.1 示例脚本 365
 - 13.2.2 无关软件 366
 - 13.2.3 开放端口 366
 - 13.2.4 未打补丁的系统 366
 - 13.3 UNIX基础 367

<<黑客>>

- 13.3.1 重要命令 367
- 13.3.2 文件许可 368
- 13.3.3 Inetd 369
- 13.3.4 Netstat 371
- 13.3.5 Tripwire 371
- 13.3.6 TCP Wrappers 372
- 13.3.7 Lsof 372
- 13.3.8 Suid 373
- 13.4 小结 373
- 第14章 UNIX攻击 374
 - 14.1 UNIX攻击 374
 - 14.1.1 Aglimpse 374
 - 14.1.2 Campas 378
 - 14.1.3 NetPR 380
 - 14.1.4 DTprintinfo 389
 - 14.1.5 Sadmin攻击 397
 - 14.1.6 XWindows 402
 - 14.1.7 Solaris Catman Race Condition漏洞 412
 - 14.1.8 Multiple Linux Vendor RPC.STATD攻击 412
 - 14.2 小结 414
- 第15章 保留访问权限 415
 - 15.1 后门和特洛伊木马程序 416
 - 15.1.1 QAZ 417
 - 15.1.2 后门监听代理 417
 - 15.2 Rootkit 418
 - 15.2.1 文件级Rootkit 419
 - 15.2.2 内核级Rootkit 420
 - 15.2.3 NT Rootkit 420
 - 15.2.4 UNIX Rootkit 421
 - 15.3 NT后门 423
 - 15.3.1 Brown Orifice攻击 423
 - 15.3.2 Donald Dick 1.55 428
 - 15.3.3 SubSeven 435
 - 15.3.4 Back Orifice 443
 - 15.3.5 包装程序 445
 - 15.4 小结 445
- 第16章 隐藏踪迹 447
 - 16.1 隐藏攻击踪迹的方法 447
 - 16.1.1 日志文件 448
 - 16.1.2 文件信息 460
 - 16.1.3 附加文件 462
 - 16.1.4 隐藏网络上的踪迹 463
 - 16.2 小结 465
- 第17章 其他类型的攻击 466
 - 17.1 Bind 8.2 NXT攻击 466
 - 17.1.1 攻击细节 466
 - 17.1.2 协议描述 466

<<黑客>>

- 17.1.3 变种描述 467
- 17.1.4 攻击原理 467
- 17.1.5 使用方法 468
- 17.1.6 攻击特征 469
- 17.1.7 防范措施 471
- 17.1.8 源代码/伪代码 471
- 17.2 Cookie攻击 471
 - 17.2.1 攻击细节 472
 - 17.2.2 CGI协议描述 472
 - 17.2.3 CGI协议工作原理 472
 - 17.2.4 CGI协议弱点 472
 - 17.2.5 Cookie协议描述 472
 - 17.2.6 Cookie协议工作原理 473
 - 17.2.7 Cookie协议弱点 473
 - 17.2.8 攻击原理 473
 - 17.2.9 成功原因 473
 - 17.2.10 攻击图解 474
 - 17.2.11 攻击特征 474
 - 17.2.12 怎样防止攻击 475
 - 17.2.13 防范措施 475
 - 17.2.14 源代码/伪代码 475
- 17.3 SNMP 团体字符串 479
 - 17.3.1 攻击细节 479
 - 17.3.2 协议描述 479
 - 17.3.3 历史回溯 479
 - 17.3.4 SNMP结构 480
 - 17.3.5 SNMP消息 480
 - 17.3.6 SNMP验证 482
 - 17.3.7 攻击原理 482
 - 17.3.8 使用方法 482
 - 17.3.9 攻击特征 487
 - 17.3.10 防范措施 487
 - 17.3.11 攻击图解 488
 - 17.3.12 源代码/伪代码 488
 - 17.3.13 脆弱的设备 489
 - 17.3.14 附加信息 489
- 17.4 Sniffing与Dsniff 490
 - 17.4.1 攻击细节 490
 - 17.4.2 协议描述 490
 - 17.4.3 攻击变种 490
 - 17.4.4 回顾 491
 - 17.4.5 详细描述 491
 - 17.4.6 使用Dsniff及其应用 492
 - 17.4.7 进行攻击 494
 - 17.4.8 攻击特征 495
 - 17.4.9 防范措施 495
 - 17.4.10 源代码/伪代码 496

<<黑客>>

- 17.4.11 附加信息 496
- 17.5 PGP ADK攻击 496
 - 17.5.1 攻击细节 496
 - 17.5.2 协议描述 497
 - 17.5.3 攻击原理 498
 - 17.5.4 攻击图解 504
 - 17.5.5 使用方法 504
 - 17.5.6 攻击特征 507
 - 17.5.7 防范措施 509
 - 17.5.8 附加信息 510
- 17.6 Cisco IOS口令脆弱性 510
 - 17.6.1 攻击细节 510
 - 17.6.2 Cisco IOS的概念 510
 - 17.6.3 Cisco IOS口令的不同种类 511
 - 17.6.4 攻击原理 512
 - 17.6.5 使用方法 515
 - 17.6.6 攻击特征 516
 - 17.6.7 防范措施 516
 - 17.6.8 源代码/伪代码 517
 - 17.6.9 附加信息 518
- 17.7 针对密钥交换的Man-in-the-Middle攻击 518
 - 17.7.1 攻击细节 518
 - 17.7.2 回顾 519
 - 17.7.3 协议描述 519
 - 17.7.4 基本注意事项 520
 - 17.7.5 Otway-Rees密钥交换协议规范 520
 - 17.7.6 攻击原理 522
 - 17.7.7 变种描述 523
 - 17.7.8 使用方法 524
 - 17.7.9 攻击特征 525
 - 17.7.10 防范Otway-Rees密钥交换协议攻击的措施 526
 - 17.7.11 源代码 527
 - 17.7.12 伪代码 527
 - 17.7.13 附加信息 528
- 17.8 HTTP Tunnel攻击 528
 - 17.8.1 攻击细节 528
 - 17.8.2 协议描述 528
 - 17.8.3 攻击机制 530
 - 17.8.4 实施攻击 530
 - 17.8.5 攻击特征 530
 - 17.8.6 建议 531
 - 17.8.7 附加信息 531
- 17.9 小结 531
- 第18章 SANS十大漏洞 533
 - 18.1 SANS列出的十种漏洞 533
 - 18.1.1 BIND漏洞会使Root权限被马上攻克 534
 - 18.1.2 脆弱的CGI程序和程序扩展 535

<<黑客>>

- 18.1.3 远程过程调用漏洞 537
- 18.1.4 RDS安全漏洞 538
- 18.1.5 Sendmail缓冲区溢出漏洞 538
- 18.1.6 Sadmin和Mountd 539
- 18.1.7 基于NetBIOS的全局文件共享和不适当信息共享 540
- 18.1.8 无口令或口令脆弱的User ID, 特别是root/管理员 541
- 18.1.9 IMAP和POP缓冲区溢出漏洞或不正确设置 542
- 18.1.10 设为Public和Private的默认SNMP团体字符串 543
- 18.1.11 附: Internet Explorer和Office 2000中的诸多脚本漏洞 543
- 18.2 经常被探测的端口 544
- 18.3 根据SANS Top 10列表来判断脆弱性 545
- 18.4 小结 546
- 第19章 回顾 547
 - 19.1 攻击详述 547
 - 19.1.1 场景1——Rogue调制解调器 548
 - 19.1.2 场景2——社会工程 549
 - 19.1.3 场景3——安全的物理破坏 549
 - 19.1.4 场景4——攻击NT 550
 - 19.1.5 场景5——攻击UNIX 550
 - 19.2 小结 551
- 第20章 总结 552
 - 20.1 安全不容忽视 552
 - 20.2 保护站点的一般技巧 553
 - 20.2.1 最少权限原则 555
 - 20.2.2 了解系统运行的程序 555
 - 20.2.3 防范是目标, 探测是必须 555
 - 20.2.4 安装最新的补丁 556
 - 20.2.5 定期的系统检测 556
 - 20.3 情况越来越糟 556
 - 20.4 未来尚未可知 557
 - 20.4.1 安全破坏会增加 557
 - 20.4.2 重大安全事件发生的必然性 557
 - 20.4.3 厂商会生产安全的产品 559
 - 20.4.4 公司会以安全为重点 560
 - 20.4.5 我们将会拥有一个安全的世界 560
 - 20.5 小结 560
- 附录A 参考资料 561

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>