

<<Windows 2000黑客大曝光>>

图书基本信息

书名：<<Windows 2000黑客大曝光>>

13位ISBN编号：9787302058489

10位ISBN编号：7302058482

出版时间：2002-10-1

出版时间：清华大学出版社

作者：Joel Scambray,Stuart McClure

页数：497

字数：626

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>

## <<Windows 2000黑客大曝光>>

### 内容概要

本书内容包括：网络和系统的概念及Windows 2000的安全体系；网络中发现和探测目标的技术和防御方法；入侵和占领整个系统、扩展权限、清除作案痕迹的方法以及相应的防御措施；IIS5, SQL Server, 终端服务器, Internet客户端的攻击技术以及物理攻击、拒绝服务攻击；Windows 2000的安全工具。

全书注重案例分析，讲解了很多具体攻击的过程，更重要的是对几乎所有讨论过的攻击手段都提供了相应的对策。

本书是安全漏洞的宝典，是负责安全保障工作的网络管理员和系统管理员的必读之书，也可作为信息管理员以及对计算机和网络安全感兴趣的人员的重要参考书。

## <<Windows 2000黑客大曝光>>

### 作者简介

Joel Scambray是国际畅销的Internet安全系列丛书《黑客大曝光》(<http://www.hackingexposed.com>)的作者之一。

该书在2001年已出版了第3版。

Joel多年的IT安全顾问经历成为他写作的主要来源。

他的客户既包括“财富50强”中的企业，也有新成立的公司，从中他获得了关于各种安全技术的大量经过实际检验的知识，他曾经设计和分析过各种应用程序和产品的安全架构。

Joel为多个组织提供Windows 2000安全咨询服务，包括计算机安全协会、MIS培训协会、SANS(系统管理、网络与安全协会)、ISSA(信息系统安全协会)、ISACA(信息系统审计与控制协会)和很多大型企业，他还一直担任Foundstone公司“Windows终极黑客”课程的主讲。

现在他是Foundstone公司(<http://www.foundstone.com>)的高层管理人员，在此之前曾任Ernst & Young公司的经理、Infoworld公司的测试中心高级分析员和一家大型商业房地产公司的IT主管。

Joel的学历背景包括加利福尼亚大学洛杉矶分校(UCLA)的高级学位，并且持有信息系统安全专家认证(CISSP)证书。

——Joel Scambray的联系方式：[joel@hackingexposed.com](mailto:joel@hackingexposed.com)

Stuart McClure

Stuart十余年的IT和安全工作经历为《黑客大曝光》系列带来了丰富的内容。

他是这本书的创建者之一，并帮助推进本书成为国际上空前畅销的网络安全书籍。

Stuart也是“安全观察”(<http://www.infoworld.com/security>)的合作创建者，这个每周专栏自1998年来曾多次提出重要的安全问题、漏洞和弱点。

目前Stuart是一流的安全评估、咨询、培训和技术公司Foundstone的董事长、首席技术官。

在参与创建Foundstone之前，Stuart是Ernst & Young公司安全配置服务组的高级经理，负责项目管理、攻击、入侵评审和技术鉴定。

他曾经担任过的职位包括Infoworld测试中心的安全分析员，曾评估过近100个网络和安全产品，特别是防火墙、安全审核、入侵检测和公钥体系(PKI)产品。

在进入Infoworld之前，Stuart曾在其他公司的IT部门任网络、系统和安全管理员，管理Novell、NT、Solaris、AIX和AS/400等平台超过6年之久。

Stuart持有科罗拉多玻尔大学的学士学位和多种认证证书，包括ISC2的CISSP(信息系统安全专家认证)、Novell的CNE(认证网络工程师)和Check Point的CCSE(认证安全管理员)。

——Stuart McClure的联系方式：[stuart@hackingexposed.com](mailto:stuart@hackingexposed.com)

关于技术审阅者

Chip Andrews

Chip Andrews是Clarus公司的软件安全设计师，有超过12年的软件开发经验。

他为《Microsoft Certified Professional》和《SQL Server Magazine》等杂志撰过写关于SQL安全性和软件开发问题的文章。

Chip曾多次在与Microsoft SQL Server安全问题和安全应用程序设计有关的会议上发表演讲。

Erik Pace Birkholz, CISSP

Erik是Foundstone的首席顾问。

Erik的主要研究领域是Internet和Intranet技术以及它们所包含的协议、网络设备和操作系统的安全问题。

他主要关注攻击和渗透测试以及安全架构设计。

## <<Windows 2000黑客大曝光>>

Erik还是Foundstone公司的“终极黑客：动手做”和“终极NT/2000安全：动手做”课程的主讲。在加入Foundstone公司之前，他是Internet安全系统公司(ISS)的西海岸顾问组的评估主管。在ISS之前，Erik为Ernst & Young公司的eSecurity服务部门工作。他是国家攻击和渗透小组的成员，“极端黑客”课程的讲师。Erik还在国家计算机安全协会(NSCA)从事了两年的研究分析员。

Erik对国际畅销书《黑客大曝光》作出了重要的贡献，他的研究成果还发表在国家计算机安全协会期刊和Foundstone的“数字战场”上。他还在Black Hat简报和Internet安全会议(TISC)上报告了他的研究。

Erik持有宾夕法尼亚Dickinson学院的学士学位，曾获1999-2000年度优秀毕业生奖“Metzger Conway Fellow”。他持有认证信息系统安全专家(CISSP)和Microsoft认证系统工程师(MCSE)证书。

### Clinton Mugge

Clinton Mugge是为Foundstone的客户提供信息安全咨询服务的首席管理顾问，专门负责网络评估、产品测试和安全架构。他持有认证信息系统安全专家(CISSP)证书。

Mugge有7年的安全工作经验，涉及物理安全、主机、网络架构和间谍事件调查。他曾与政府机构和众多IT公司进行过联合政府调查、突发事件响应项目和网络评估工作。在加入Foundstone之前，Mugge为Ernst & Young公司工作，后来又任美国陆军反情报官员。Mugge多次在会议上发表演讲、为专栏撰写文章，还是Osborne/McGraw-Hill出版的《突发事件响应》一书的技术评论。Mugge持有计算机管理学士学位和市场营销学士学位。

——Clinton Mugge的联系方式：[clinton.mugge@foundstone.com](mailto:clinton.mugge@foundstone.com)

### Eric Schultze

Eric Schultze在过去的9年中一直从事信息技术和安全工作，大部分时间关注于评估和保护Microsoft技术和平台。

他经常在信息会议上发表演讲，包括NetWorld+Interop、Usenix、BlackHat、SANS和MIS，是计算机安全协会的教师。

Schultze还经常出现在电视和多种媒体上，包括NBC、CNBC、TIME、ComputerWorld和The Standard。Schultze曾为Foundstone、SecurityFocus.com、Ernst&Young、Price Waterhouse、Bealls和Salomon Brothers公司工作。

他是《黑客大曝光》第一版的作者之一，目前是Microsoft公司的安全程序经理。

### David Wong

David是计算机安全专家，Foundstone公司的首席顾问。

他进行过大量的安全产品评测以及网络攻击和渗透测试。

David在进入Foundstone之前是大型电讯公司的软件工程师，负责开发进行网络侦察和监视的软件。

# <<Windows 2000黑客大曝光>>

## 书籍目录

序

前言

第1部分 基础知识

第1章 网络和系统安全基础 3

1.1 基本的安全实践 4

1.2 小结 7

1.3 参考和深入阅读 7

第2章 黑客眼中的Windows 2000安全架构 9

2.1 Windows 2000安全模型 10

2.2 安全主体 12

2.2.1 用户 12

2.2.2 组 13

2.2.3 特殊身份 15

2.2.4 其他安全主体和容器 15

2.2.5 SAM和活动目录 16

2.3 森林、树、域 17

2.3.1 作用域：本地、全局、通用 18

2.3.2 信任 19

2.3.3 管理边界：是森林还是域 19

2.4 SID 22

2.5 综合：认证和授权 24

2.5.1 令牌 25

2.5.2 网络认证 27

2.6 审核 29

2.7 小结 30

2.8 参考和深入阅读 32

第2部分 侦察

第3章 踩点和扫描 37

3.1 踩点 38

3.2 扫描 43

3.3 连续进行踩点和扫描的重要性 53

3.4 小结 53

3.5 参考和深入阅读 53

第4章 查点 55

4.1 序幕：回顾扫描的结果 56

4.2 NetBIOS网络查点 58

4.3 Windows 2000 DNS查点 64

4.4 SNMP查点 81

4.5 活动目录查点 85

4.6 小结 89

4.7 参考和深入阅读 91

第3部分 分而治之

第5章 CIFS/SMB攻击 95

5.1 猜测SMB密码 96

5.1.1 关闭与目标之间的空连接 97

## <<Windows 2000黑客大曝光>>

- 5.1.2 回顾查点结果 97
- 5.1.3 避免账户锁定 98
- 5.1.4 Administrator和服务账户的重要性 100
- 5.2 窃听SMB认证 113
- 5.3 小结 128
- 5.4 参考和深入阅读 129
- 第6章 权限提升 133
- 6.1 命名管道预测 134
- 6.2 作为SYSTEM身份运行的NetDDE 137
- 6.3 权限提升的一般对策 139
- 6.4 小结 141
- 6.5 参考和深入阅读 141
- 第7章 获得交互 143
- 7.1 命令行控制 144
- 7.2 图形用户界面(GUI)控制 152
- 7.3 小结 154
- 7.4 参考和深入阅读 154
- 第8章 扩大影响 157
- 8.1 审核 158
- 8.2 密码提取 160
- 8.2.1 获取可逆加密的密码 161
- 8.2.2 从LSA缓存中获取明文密码 161
- 8.3 密码破解 163
- 8.4 文件搜索 171
- 8.5 GINA木马 176
- 8.6 嗅探 178
- 8.7 中继跳板 180
- 8.8 端口重定向 185
- 8.9 小结 188
- 8.10 参考和深入阅读 188
- 第9章 清除痕迹 191
- 9.1 创建虚假用户账户 192
- 9.2 木马登录屏幕 193
- 9.3 远程控制 193
- 9.4 在哪里放置后门和木马 195
- 9.4.1 “开始”文件夹 196
- 9.4.2 “开始”注册表主键 196
- 9.4.3 驱动程序 197
- 9.4.4 利用Web浏览器启动页面下载代码 197
- 9.4.5 计划任务 198
- 9.5 rootkit 198
- 9.6 掩盖踪迹 200
- 9.6.1 清除日志 200
- 9.6.2 隐藏文件 201
- 9.7 通用对策：小型的公开检测 205
- 9.8 小结 212
- 9.9 参考和深入阅读 212

## &lt;&lt;Windows 2000黑客大曝光&gt;&gt;

## 第4部分 攻击脆弱服务和客户端

## 第10章 攻击IIS 5和Web应用程序 217

## 10.1 攻击 IIS 5 218

## 10.1.1 IIS攻击基础 218

## 10.1.2 IIS 5缓冲区溢出 224

## 10.1.3 文件系统遍历 235

## 10.1.4 将文件写入Web服务器 243

## 10.1.5 通过IIS 5提升权限 248

## 10.1.6 源代码泄露攻击 252

## 10.2 Web服务器安全评估工具 264

## 10.2.1 Stealth HTTP Scanner 265

## 10.2.2 SSLProxy 265

## 10.2.3 Achilles 266

## 10.2.4 wfetch 267

## 10.2.5 whisker 268

## 10.3 攻击Web应用程序 270

## 10.4 小结 273

## 10.5 参考和深入阅读 277

## 第11章 攻击SQL Server 283

## 11.1 案例研究：SQL Server渗透 284

## 11.2 SQL Server的安全概念 288

## 11.2.1 网络库 286

## 11.2.2 安全模式 289

## 11.2.3 登录 290

## 11.2.4 用户 290

## 11.2.5 角色 290

## 11.2.6 日志 291

## 11.2.7 SQL Server 2000的改进 292

## 11.3 入侵SQL Server 293

## 11.3.1 SQL Server信息收集 293

## 11.3.2 SQL Server入侵工具和技术 296

## 11.3.3 SQL Server的已知漏洞 306

## 11.3.4 SQL代码注入攻击 310

## 11.3.5 违规利用SQL扩展存储过程以操作Windows 2000 315

## 11.4 SQL Server的最佳安全操作 319

## 11.5 小结 323

## 11.6 参考和深入阅读 324

## 第12章 攻击终端服务器 327

## 12.1 终端服务器基础 328

## 12.1.1 服务器 329

## 12.1.2 远程桌面协议(RDP) 329

## 12.1.3 客户端 329

## 12.2 识别和查点TS 330

## 12.3 攻击TS 333

## 12.3.1 防御 337

## 12.3.2 终端服务器安全基础 338

## 12.3.3 终端服务器高级安全功能 340

## &lt;&lt;Windows 2000黑客大曝光&gt;&gt;

- 12.4 小结 341
- 12.5 参考和深入阅读 341
- 第13章 攻击Microsoft Internet客户端 343
  - 13.1 攻击类型 344
  - 13.2 实现Internet客户端攻击 345
    - 13.2.1 恶意Web页面 345
    - 13.2.2 恶意电子邮件 346
    - 13.2.3 恶意新闻组/列表文章 348
  - 13.3 攻击 349
    - 13.3.1 缓冲区溢出 349
    - 13.3.2 执行命令 354
    - 13.3.3 写本地文件 357
    - 13.3.4 有效负载：VBS地址簿蠕虫 362
    - 13.3.5 读取本地文件 365
    - 13.3.6 调用客户端出站连接 368
  - 13.4 综合：一次完整的客户端攻击 370
  - 13.5 通用对策 374
    - 13.5.1 为什么不放弃Microsoft Internet客户端 376
    - 13.5.2 IE Security Zone 377
    - 13.5.3 客户端和服务器的病毒预防 383
    - 13.5.4 基于网关的内容过滤 384
  - 13.6 小结 385
  - 13.7 参考和深入阅读 385
- 第14章 物理攻击 391
  - 14.1 对SAM进行离线攻击 392
  - 14.2 对EFS的影响 395
  - 14.3 小结 402
  - 14.4 参考和深入阅读 403
- 第15章 拒绝服务 405
  - 15.1 当前的Windows 2000 DoS攻击 407
  - 15.2 防御DoS的最佳操作 416
    - 15.2.1 最佳操作 416
    - 15.2.2 针对Windows 2000 DoS的建议 417
  - 15.3 小结 420
  - 15.4 参考和深入阅读 420
- 第5部分 防御
- 第16章 Windows 2000安全功能和工具 425
  - 16.1 安全模板、安全配置和分析 426
    - 16.1.1 安全模板 427
    - 16.1.2 安全配置和分析 429
  - 16.2 组策略 431
    - 16.2.1 已定义组策略 431
    - 16.2.2 使用组策略 432
    - 16.2.3 如何应用组策略 434
  - 16.3 IPSec 435
    - 16.3.1 IPSec过滤器的优点 436
    - 16.3.2 IPSec过滤的现有限制 436



## <<Windows 2000黑客大曝光>>

- 16.3.3 逐步创建IPSec策略 441
- 16.3.4 使用ipsecpol在命令行中管理过滤器 447
- 16.3.5 IPSec工具 449
- 16.4 Kerberos 450
- 16.5 加密文件系统 451
- 16.6 RUNAS 452
- 16.7 Windows文件保护 454
- 16.8 小结 456
- 16.9 参考和深入阅读 456
- 第17章 Windows 2000的未来 459
- 17.1 Windows的未来：路标 460
- 17.2 .NET Framework 460
  - 17.2.1 通用语言运行时(CLR) 461
  - 17.2.2 框架类 462
  - 17.2.3 ASP.NET 462
- 17.3 代号Whistler 462
  - 17.3.1 Whistler的版本 463
  - 17.3.2 Whistler的安全功能 463
  - 17.3.3 原始套接字和其他未经证实的声明 473
- 17.4 小结 473
- 17.5 参考和深入阅读 474
- 第6部分 附录
- 附录A Windows 2000安全检查清单 475
  - A.1 自行负责：角色和责任 476
  - A.2 安装前的考虑 476
  - A.3 基本的Windows 2000加固措施 477
    - A.3.1 与模板无关的建议 477
    - A.3.2 安全模板的建议 483
    - A.3.3 IPSec过滤器 485
    - A.3.4 组策略 486
    - A.3.5 其他配置 486
  - A.4 IIS 5的安全考虑 487
  - A.5 SQL Server的安全考虑 490
  - A.6 终端服务器的安全考虑 492
  - A.7 拒绝服务的对策 493
  - A.8 Internet客户端安全性 495
  - A.9 审核你自己 496
  - A.10 参考和深入阅读 497

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>