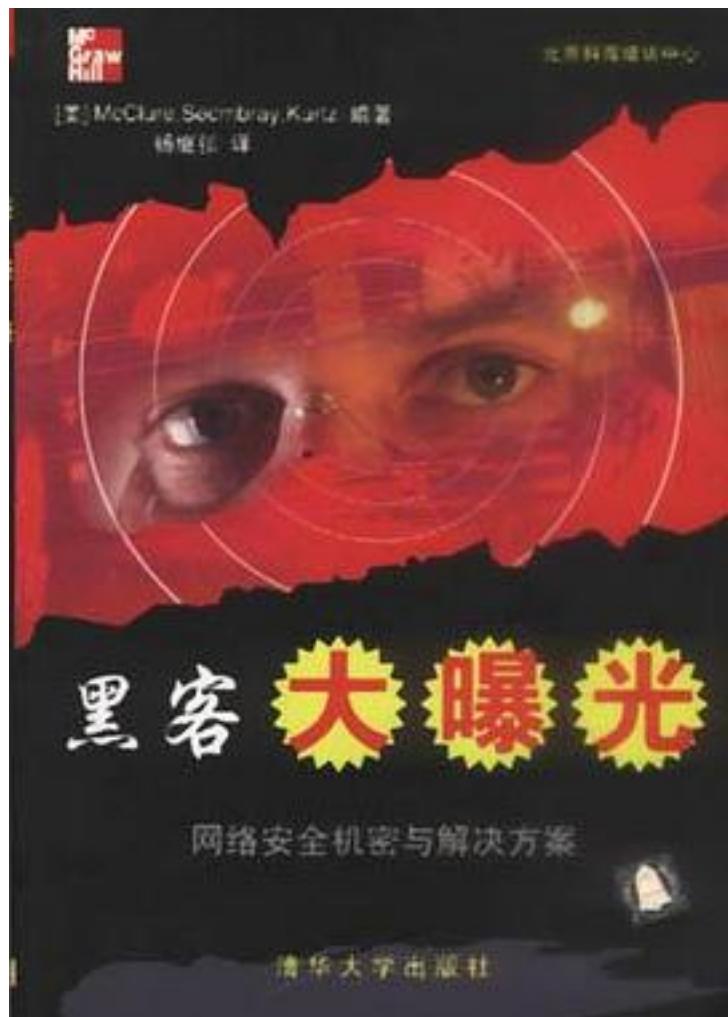


黑客大曝光



[黑客大曝光 下载链接1](#)

著者: (美) McClure

出版者:清华大学出版社

出版时间:2000-09

装帧:平装

isbn:9787302040002

本书从攻击者和防御者的不同角度，讲述了计算机和网络入侵手段与应对措施。

全书内容包括：从远程探测一个系统，标识其中的脆弱点到发掘特定操作系统（主要是Windows NT、UNIX、Novell Netware）上的漏洞的完整过程。轰炸拨打程序的应用、防火墙的规避、拒绝服务型攻击的发动、远程控制软件的滥用以及针对Web的攻击，也在本书的讨论之中。附录中还分析了windows 2000的安全特性。

本书讲解了很多具体攻击过程，解释了攻击者确切想要什么，他们如何攻溃相关的安全屏障，成功之后怎么办等内容。本书特色在于几乎所有讨论过的攻击手段都有相应的对策。

本书适合没有太多时间研究安全保障工作的网络管理员和系统管理员阅读，也可作为对计算机和网络安全感兴趣的人员参考。

作者介绍：

stuart McClure

Stuart McClure (CISSP, CNE, CCSE) 是Ernst & Young公司电子安全解决方案业务部 (eSecurity Solutions practice) 的一位高级主管。McClure先生是InfoWorld杂志安全观察 (Security Watch) 专栏的协作者，这是探讨时事性安全事务、漏洞发掘和脆弱性等内容的每期的全球性安全专栏。McClure先生有10年以上在公司、学术机构及政府部门的网络与系统安全方面配置与管理的经验。他擅长攻击与渗透方法、安全评估审查、防火墙与连网安全体系架构、紧急情况响应、入侵检测以及PKI技术。McClure先生加盟Ernst & Young公司之前的两年在InfoWorld测试中心工作，测试专门用于防火墙、安全审计、入侵检测和PKI产品的网络与安全软硬件。

Joel Scambray

Joel Scambray是Ernst & Young公司电子安全解决方案业务部的一位主管，他在那儿向各式各样的机构提供信息系统安全咨询服务，特别是在攻击与渗透测试、主机安全评估、虚拟私用网络 (VPN) 连接、产品测试以及安全体系结构的设计、实现与审计上。Joel参与编写InfoWorld杂志每期的安全观察专栏，发表了10多篇技术产品比较、评论和分析文章。他有6年以上基于操作性或策略性立场应用多种计算机和通信技术的工作经验，包括担任InfoWorld测试中心分析员的2年，以及在一家大的商业房地产公司担任IT主任的2年。

George Kurtz

George Kurtz是Ernst & Young公司电子安全解决方案业务部的一位高级主管，同时也是他们的剖析服务热线 (Profiling service line) 的全国攻击与渗透主任。Kurtz先生在他的安全咨询职业生涯中完成了数百个防火墙、网络和与电子商业相关的安全评估。Kurtz先生对于入侵检测、防火墙技术、紧急情况响应过程以及远程访问方案有相当丰富的经验。Kurtz先生是颇受赞誉的课程“极端黑客攻击手段——防御你的网点 (Extreme Hacking—Defending Your Site)”的领头教员之一。他是许多安全会议的固定发言人，并为多家出版物所引用，包括 The Wall Street Journal、InfoWorld和美联社 (the Associated Press)。Kurtz先生给多家安全相关出版物写过若干篇文章。

目录: 第1部分 窥探设施

第1章 踩点——目标探测

- 1. 1 什么是踩点
- 1. 1. 1 踩点必要性的原因
- 1. 2 因特网踩点
- 1. 2. 1 步骤1: 确定活动范围
- 1. 2. 2 步骤2: 网络查点
- 1. 2. 3 步骤3: DNS质询
- 1. 2. 4 步骤4: 网络勘察
- 1. 3 小结

第2章 扫描

- 2. 1 网络ping扫射
- 2. 1. 1 ping扫射对策
- 2. 2 ICMP查询
- 2. 2. 1 ICMP查询对策
- 2. 3 端口扫描
- 2. 3. 1 扫描类型
- 2. 3. 2 标识运行着的TCP服务和UDP服务
- 2. 3. 3 端口扫描细目
- 2. 3. 4 端口扫描对策
- 2. 4 操作系统检测
- 2. 4. 1 协议栈指纹鉴别
- 2. 4. 2 操作系统检测对策
- 2. 5 完整的春卷: 自动发现工具
- 2. 5. 1 自动发现工具对策
- 2. 6 小结

第3章 查点

- 3. 1 简介
- 3. 1. 1 Windows NT查点
- 3. 1. 2 Novell查点
- 3. 1. 3 UNIX查点
- 3. 2 小结

第4章 攻击Windows 95/98

- 4. 1 Windows 9x远程漏洞发掘
- 4. 1. 1 直接连接到Windows 9x共享资源
- 4. 1. 2 Windows 9x后门
- 4. 1. 3 已知的服务器程序脆弱点
- 4. 1. 4 Windows 9x拒绝服务
- 4. 2 从控制台攻击Windows 9x
- 4. 2. 1 绕开Windows 9x安全: 重启
- 4. 2. 2 较隐秘的方法之一: Autorun与暴露屏幕保护程序保密字
- 4. 2. 3 更为隐秘的方法之二: 揭示内存中的Windows 9x保密字
- 4. 2. 4 隐秘方法之三: 破解保密字
- 4. 3 小结

第5章 攻击Windows NT

- 5. 1 索取 Administrator账号
- 5. 1. 1 在网络上猜测保密字
- 5. 1. 2 对策: 防御保密字猜测
- 5. 1. 3 远程漏洞发掘; 拒绝服务和缓冲区溢出
- 5. 1. 4 特权升级
- 5. 2 巩固权力

- 5. 2. 1 破解 SAM
- 5. 2. 2 发掘信任漏洞
- 5. 2. 3 远程控制与后门
- 5. 2. 4 一般性后门与对策
- 5. 3 掩盖踪迹
- 5. 3. 1 禁止审计
- 5. 3. 2 清空事件登记结果
- 5. 3. 3 隐藏文件
- 5. 4 小结

第6章 攻击Novell NetWare

- 6. 1 附接但不接触
- 6. 1. 1 On-Site Admin
- 6. 1. 2 Snlist和nslist
- 6. 1. 3 附接对策
- 6. 2 查点平均数据库和NDS树
- 6. 2. 1 userinfo
- 6. 2. 2 userdump
- 6. 2. 3 finger
- 6. 2. 4 bindery
- 6. 2. 5 bindin
- 6. 2. 6 nlist
- 6. 2. 7 Cx
- 6. 2. 8 On-Site Admin
- 6. 2. 9 查点对策
- 6. 3 打开未锁的门
- 6. 3. 1 chknnull
- 6. 3. 2 chknnull对策
- 6. 4 经认证的查点
- 6. 4. 1 userlist/a
- 6. 4. 2 On-Site Admin
- 6. 4. 3 NDSsnoop
- 6. 5 检测入侵者锁闭特性
- 6. 5. 1 入侵者锁闭特性检测对策
- 6. 6 获取管理性特权
- 6. 6. 1 偷窃
- 6. 6. 2 偷窃对策
- 6. 6. 3 Nwpcrack
- 6. 6. 4 Nwpcrack对策
- 6. 7 服务器程序脆弱点
- 6. 7. 1 NetWare Perl
- 6. 7. 2 Netware Perl对策
- 6. 7. 3 Netware FTP
- 6. 7. 4 Netware FTP对策
- 6. 7. 5 NetWare Web Server
- 6. 7. 6 NetWare Web Server对策
- 6. 8 欺骗性攻击 (Pandora)
- 6. 8. 1 gameover
- 6. 8. 2 Pandora对策
- 6. 9 拥有一台服务器的管理权之后
- 6. 9. 1 rconsole攻击
- 6. 9. 2 rconsole (明文保密字) 对策
- 6. 10 攫取NDS文件
- 6. 10. 1 NetBadic. nlm

- 6. 10. 2 Dsmaint
- 6. 10. 3 Jcmd
- 6. 10. 4 攫取NDS对策
- 6. 10. 5 破解NDS文件
- 6. 11 登记结果篡改
- 6. 11. 1 关掉审计功能
- 6. 11. 2 变更文件历史
- 6. 11. 3 篡改控制台登记结果
- 6. 11. 4 登记结果篡改对策
- 6. 12 后门
- 6. 12. 1 后门对策
- 6. 13 更深入的资源
- 6. 13. 1 Kane Security Analyst
- 6. 13. 2 Web网站
- 6. 13. 3 Usenet新闻组

第7章 攻击UNIX

- 7. 1 追求root访问权
- 7. 1. 1 简短回顾
- 7. 1. 2 脆弱点映射
- 7. 2 远程访问对比本地访问
- 7. 3 远程访问
- 7. 3. 1 蛮力攻击
- 7. 3. 2 数据驱动攻击之一：缓冲区溢出
- 7. 3. 3 数据驱动攻击之二：输入验证
- 7. 3. 4 想要自己的shell
- 7. 3. 5 常用类型的远程攻击
- 7. 4 本地访问
- 7. 4. 1 保密字构造脆弱点
- 7. 4. 2 本地缓冲区溢出
- 7. 4. 3 符号链接
- 7. 4. 4 文件描述字攻击
- 7. 4. 5 竞争状态
- 7. 4. 6 core文件操纵
- 7. 4. 7 共享函数库
- 7. 4. 8 系统误配置
- 7. 4. 9 shell攻击
- 7. 5 获取root特权之后
- 7. 5. 1 root 工具箱
- 7. 5. 2 特洛伊木马
- 7. 5. 3 嗅探程序
- 7. 5. 4 登记结果清理
- 7. 6 小结

第3部分 攻击网络

第8章 拨号攻击与VPN

- 8. 1 电话号码踩点
- 8. 1. 1 对策：阻止信息的泄漏
- 8. 2 战术拨号
- 8. 2. 1 硬件
- 8. 2. 2 合法性问题
- 8. 2. 3 外围
- 8. 2. 4 软件

- 8. 2. 5 载波漏洞发掘技巧
- 8. 2. 6 拨号安全措施
- 8. 3 虚拟私用连网 (VPN) 攻击
- 8. 4 小结

第9章 网络设备

- 9. 1 发现
- 9. 1. 1 检测
- 9. 1. 2 SNMP
- 9. 2 后门
- 9. 2. 1 缺省账号
- 9. 2. 2 网络设备脆弱点
- 9. 3 共享式媒体对比交换式媒体
- 9. 3. 1 检测自己所在的媒体
- 9. 3. 2 捕捉SNMP信息
- 9. 4 SNMP set请求
- 9. 4. 1 SNMP set请求对策
- 9. 5 RIP欺骗
- 9. 5. 1 RIP欺骗对策
- 9. 6 小结

第10章 防火墙

- 10. 1 防火墙概貌
- 10. 2 防火墙标识
- 10. 2. 1 直接扫描：嘈杂的技巧
- 10. 2. 2 路径跟踪
- 10. 2. 3 旗标攫取
- 10. 2. 4 使用nmap简单推断
- 10. 2. 5 端口标识
- 10. 3 穿透防火墙扫描
- 10. 3. 1 hping
- 10. 3. 2 firewalk工具
- 10. 4 分组过滤
- 10. 4. 1 自由散漫的ACL规则
- 10. 4. 2 CheckPoint诡计
- 10. 4. 3 ICMP和UDP隧道
- 10. 5 应用代理脆弱点
- 10. 5. 1 主机名：localhost
- 10. 5. 2 未加认证的外部代理访问
- 10. 5. 3 WinGate脆弱点
- 10. 6 小结
- • • • • (收起)

[黑客大曝光](#) [下载链接1](#)

标签

黑客

网络安全

信息安全

评论

一本很有意思的案例书

[黑客大曝光 下载链接1](#)

书评

[黑客大曝光 下载链接1](#)